

# Handreiking DDoS aangifte

Vragen of opmerkingen over deze handreiking? Neem contact op: [cybercrime.opsporing.midden-nederland@politie.nl](mailto:cybercrime.opsporing.midden-nederland@politie.nl)

Deze handreiking is bedoeld ter ondersteuning bij het opnemen van een aangifte van DDoS en/of dreiging van DDoS. Voor het succesvol onderzoeken van een aangifte is het belangrijk dat de politie zoveel mogelijk relevante informatie heeft over **de aanval**, het **contact met een mogelijke afperser/aanvaller** en de **IT-situatie van een bedrijf** (website, bedrijfsnetwerk, etc).

Onderaan deze handreiking staat meer uitleg over **DDoS**, **strafbaarheid** en een **woordenlijst** met korte uitleg van termen.

De gevraagde informatie is van cruciaal belang om een **mogelijke dader** te vinden en berechten. Twijfel je of informatie voor de aangifte van belang is, maar is het wel beschikbaar? Voeg het dan toch bij.

Let op: sommige van onderstaande vragen zijn technisch van aard. Waarschijnlijk moet een aangever deze informatie vragen aan de IT-organisatie of webhoster. Benadruk het belang van deze technische details: juist deze technische informatie kan ons veel vertellen over de dader en aanknopingspunten geven voor onderzoek! De gegevens van de IT partij worden dus ook uitgevraagd. Laat de aangever de IT partij hiervan op de hoogte stellen en vragen om hun medewerking.

## Benodigde informatie aangifte

### Personalia aangever

- Voornamen
- Achternaam
- Geboortedatum
- Adres
- E-mailadres aangever
- Telefoonnummer

### Gegevens benadeelde

- Naam bedrijf
- Adres
- Vestigingsplaats
- KVK-nummer
- E-mailadres
- Telefoonnummer

### Gegevens IT-partij benadeelde

- Naam contactpersoon
- E-mailadres
- Telefoonnummer
- Naam bedrijf (indien externe partij)
- Adres (indien externe partij)
- Vestigingsplaats (indien externe partij)
- KVK-nummer (indien externe partij)

### Gegevens DDoS aanval

- Korte tekstuele uitleg van wat er heeft plaatsgevonden
- Hoe veel aanvallen zijn er uitgevoerd en/of geregistreerd?

- Is een patroon te herkennen in de aanvallen? (bv. Zelfde tijdstip, of zelfde contactwijze, zelfde technische benadering, etc.)
- Is er ooit eerder (langer geleden) een vergelijkbare aanval uitgevoerd?
- Hoe zit de aangevallen infrastructuur in elkaar? Bijvoorbeeld netwerkconfiguratie, applicaties? (zie ook kopje technische informatie)
  - Welke beschermende maatregelen zijn er getroffen?
  - Wat is het zwakke punt in de infrastructuur?

#### Communicatie met een eventuele verdachte

- Is/zijn de aanval(len) opgeëist?
  - Zo ja, door wie?
  - Is er een reden gegeven voor de aanval(len)?
  - Welk medium is gebruikt om de aanval(len) op te eisen? (bv email, social media, etc.)
    - Is dit vastgelegd en zo ja, kan dit aangeleverd worden?
  - Is er contact opgenomen met de opeisende partij?
    - Zo ja, hoe heeft dat contact plaatsgevonden? Met welke gegevens (accountnaam, etc.)?
    - Is er op dit moment nog contact met de opeisende partij?
    - Indien mogelijk zoveel mogelijk correspondentie als bijlage bij de aangifte opnemen. Neem ook de technische details op, zoals de **e-mailheaders** & logging van de webserver rondom alle contactmomenten.
- Is er open bronnen onderzoek gedaan om te kijken of de aanval opgeëist is?
- Indien de aanval niet is opgeëist: heeft de aangever wellicht toch een vermoeden door wie de aanval is uitgevoerd?
  - Wat is het belang van deze persoon bij de aanval, volgens de aangever?
- Is er gedreigd met een (grotere) aanval (m.a.w.: is er sprake van afpersing/afdreigen)?
  - Zo ja, is het dreigement uitgevoerd?
  - Werde er een geldbedrag geëist?
    - Zo ja, welk bedrag werd geëist en in welke valuta? (bijv. Bitcoin)
    - Is er een tegenrekening (bijv. Bitcoin adres) bekend waaraan betaald moest worden?
    - Is er betaald?
      - Zo ja, hoe heeft de overdracht plaatsgevonden?
    - Is er een tx-hash bekend (transactiegegevens die vastgelegd zijn in de blockchain, waaruit de betaling te herleiden is)
    - Indien er op een andere wijze betaald moest worden, op welke wijze was dit en wat zijn hier de nadere betalingsdetails van?
  - Werden er andere eisen gesteld?
    - Zo ja, wat werd er geëist?
    - Is er aan de eis(en) voldaan?
  - Vond er communicatie met de eiser(s) plaats?
    - Zo ja, hoe heeft dat contact plaatsgevonden? Met welke gegevens (accountnaam, etc.)?
    - Is er op dit moment nog contact met de eiser(s)?
    - Indien mogelijk zoveel mogelijk correspondentie als bijlage bij de aangifte opnemen. Indien mogelijk ook de **e-mailheaders** en/of logging van de webserver van alle contactmomenten.

#### Schade

- Hoeveel schade is er geleden (incl. onderbouwing. Dit i.v.m. het voegen in het eventuele strafproces)?
  - In het geval van afpersing: is er betaald, en hoeveel?
  - In het geval van uitval van dienstverlening: wat zijn de gederfde inkomsten en/of wat is de overige schade?
    - Is er onderzoek verricht waarvoor kosten gemaakt zijn?
    - Zijn er remediation kosten gemaakt?
    - Zijn er kosten bekend van NAWAS/Cloudflare?
  - In het geval van gederfde inkomsten, hoelang is de website/shop onbereikbaar geweest.
    - Was dit tijdens een piekperiode (zodat potentiële klanten naar een andere site gegaan zijn en niet later alsnog bij de aangever een aankoop hadden kunnen doen)?

Welke andere relevante informatie is er verder om de geleden schade zo goed mogelijk in te schatten?

#### **Technische informatie**

- Zijn er incidentrapporten beschikbaar met betrekking tot de aanval(len)? (Bijvoorbeeld van een mitigatie provider of ISP)
  - Indien beschikbaar, graag een kopie bij de aangifte voegen en het origineel goed bewaren.
- Welke soort (type en/of layer) aanval is dit geweest?
  - Indien het om een Layer7 (Application Layer) aanval gaat, is er een unieke cookie of andere id meegestuurd?
- Is er netwerkverkeer (Bijvoorbeeld PCAP-data of netflow-data) van de aanval(len) beschikbaar?
  - Indien beschikbaar, deze data graag goed bewaren ten behoeve van een eventueel strafrechtelijk onderzoek.
- Is er bekend uit welk netwerkdeel de aanval afkomstig is? (bijv. een specifieke hoster uit Rusland). De Uplink Hoster kan dit mogelijk indicatief aangeven.
- Is er (toegangs)logging beschikbaar van langere tijd rond (voor/tijdens/na) de aanval? (Vaak doet een aanvaller vooronderzoek en wil een aanvaller controleren of de website nog bereikbaar is, dus of de aanval werkt).
- Is er andere voor het onderzoek relevante informatie beschikbaar?
  - Indien beschikbaar, wat betreft het voor informatie?
  - Deze informatie graag bij de aangifte voegen indien mogelijk. Als het niet mogelijk is om de informatie bij de aangifte te voegen, deze informatie graag goed bewaren ten behoeve van een eventueel strafrechtelijk onderzoek.

# Technische details van de aanval(len)

## Aanval 1

Start datum en tijd van de aanval (inclusief de tijdzone)	
Eind datum en tijd van de aanval (inclusief de tijdzone)	
Omvang van de datapakketten	
Hoogst aantal datapakketten per seconde	
Bandbreedte van de aanval	
Type aanvalsverkeer	
TCP- of UDP-flags	
Bron IP-adres(sen)	Graag toevoegen als bijlage (het gaat meestal om grote aantallen)!
Bron poortnummer(s)	Graag toevoegen als bijlage!
Aangevallen IP-adres(sen)	
Aangevallen poortnummer(s)	
Aangevallen service(s)	
Periode van onbeschikbaarheid van de service(s)	
Geleden schade bij deze aanval in euro's (leg uit)	

## Aanval 2

Start datum en tijd van de aanval (inclusief de tijdzone)	
Eind datum en tijd van de aanval (inclusief de tijdzone)	
Omvang van de datapakketten	
Hoogst aantal datapakketten per seconde	
Bandbreedte van de aanval	
Type aanvalsverkeer	
TCP- of UDP-flags	

Bron IP-adres(sen)	Graag toevoegen als bijlage (het gaat meestal om grote aantallen)!
Bron poortnummer(s)	Graag toevoegen als bijlage!
Aangevallen IP-adres(sen)	
Aangevallen poortnummer(s)	
Aangevallen service(s)	
Periode van onbeschikbaarheid van de service(s)	
Geleden schade bij deze aanval in euro's (leg uit)	

#### Aanval ...

Start datum en tijd van de aanval (inclusief de tijdzone)	
Eind datum en tijd van de aanval (inclusief de tijdzone)	
Omvang van de datapakketten	
Hoogst aantal datapakketten per seconde	
Bandbreedte van de aanval	
Type aanvalsverkeer	
TCP- of UDP-flags	
Bron IP-adres(sen)	Graag toevoegen als bijlage (het gaat meestal om grote aantallen)!
Bron poortnummer(s)	Graag toevoegen als bijlage!
Aangevallen IP-adres(sen)	
Aangevallen poortnummer(s)	
Aangevallen service(s)	
Periode van onbeschikbaarheid van de service(s)	
Geleden schade bij deze aanval in euro's (leg uit)	

# Toelichting (D)DoS-aanvallen en Strafbaarstelling

Vragen of opmerkingen over deze handreiking? Neem contact op: [cybercrime.opsporing.midden-nederland@politie.nl](mailto:cybercrime.opsporing.midden-nederland@politie.nl)

## Uitleg (D)DoS

### Wat is een DoS-aanval?

Een Denial of Service (DoS) is een aanval waarbij men probeert om een computer, netwerk, of dienstverlening uit te schakelen voor de gewone gebruiker of klant. Zet men hiervoor meer computers in, dan gaat het om een Distributed Denial of Service (DDoS-aanval).

### Wat is een DDoS-aanval?

Distributed Denial of Service (DDoS) is een vorm van Denial-of-Service waarbij een bepaalde dienst (bijvoorbeeld een website) niet beschikbaar wordt gemaakt door deze te bestoken met veel netwerkverkeer vanuit een groot aantal verschillende bronnen.

Meer lezen over DDoS? <https://www.politie.nl/themas/ddos.html>

Uitgebreide technische uitleg (engels): <https://www.cloudflare.com/learning/ddos/application-layer-ddos-attack/>

## Strafbaarstelling

### (D)DoS aanval

Aangifte van een of meerdere (D)DoS-aanvallen kan worden gedaan op basis van de onderstaande artikelen uit het Wetboek van Strafrecht. Er kan aangifte worden gedaan van een poging tot onderstaande feiten als de uitgevoerde (D)DoS-aanvallen geen uitval van services heeft veroorzaakt.

#### Artikel 138b

1. Met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie wordt gestraft hij die opzettelijk en wederrechtelijk de toegang tot of het gebruik van een geautomatiseerd werk belemmert door daaraan gegevens aan te bieden of toe te zenden.
2. Indien het feit wordt gepleegd met behulp van een aanzienlijk aantal geautomatiseerde werken die getroffen zijn door het gebruik van een middel als bedoeld in artikel 139d, tweede lid, dat hoofdzakelijk daarvoor geschikt is gemaakt of ontworpen, wordt de schuldige gestraft met een gevangenisstraf van ten hoogste drie jaren of een geldboete van de vierde categorie.
3. Indien het feit ernstige schade veroorzaakt, of is gepleegd tegen een geautomatiseerd werk behorende tot de vitale infrastructuur, wordt de schuldige gestraft met een gevangenisstraf van ten hoogste vijf jaren of geldboete van de vierde categorie.

#### Artikel 161sexies

Hij die opzettelijk enig geautomatiseerd werk of enig werk voor telecommunicatie vernielt, beschadigt of onbruikbaar maakt, stoornis in de gang of in de werking van zodanig werk veroorzaakt, of een ten opzichte van zodanig werk genomen veiligheidsmaatregel verijdelt, wordt gestraft:

- 1°. met gevangenisstraf van ten hoogste zes jaren of geldboete van de vijfde categorie, indien daarvan gemeen gevaar voor goederen of voor de verlening van diensten te duchten is;
- 2°. met gevangenisstraf van ten hoogste negen jaren of geldboete van de vijfde categorie, indien daarvan levensgevaar voor een ander te duchten is;

3°.met gevangenisstraf van ten hoogste vijftien jaren of geldboete van de vijfde categorie, indien daarvan levensgevaar voor een ander te duchten is en het feit iemands dood ten gevolge heeft.

### **Dreigen met (D)DoS aanval**

In het geval dat er gedreigd wordt met een of meerdere (D)DoS-aanvallen, kan aangifte worden gedaan op basis van artikel 317 lid 2 van het Wetboek van Strafrecht. Hierbij moet wel het oogmerk van de verdachte zijn om zichzelf te bevoordelen door afgifte van enig goed, schuld aangaan, etc. Dus bij alleen maar dreigen met een DDoS-aanval zonder enige voorwaarde te stellen is geen afpersing of poging daartoe.

### **Artikel 317**

1. Hij die, met het oogmerk om zich of een ander wederrechtelijk te bevoordelen, door geweld of bedreiging met geweld iemand dwingt hetzij tot de afgifte van enig goed dat geheel of ten dele aan deze of aan een derde toebehoort, hetzij tot het aangaan van een schuld of het teniet doen van een inschuld, hetzij tot het ter beschikking stellen van gegevens, wordt, als schuldig aan afpersing, gestraft met gevangenisstraf van ten hoogste negen jaren of geldboete van de vijfde categorie.
2. Met dezelfde straf wordt gestraft hij die de dwang, bedoeld in het eerste lid, uitoefent door de bedreiging dat gegevens die door middel van een geautomatiseerd werk zijn opgeslagen, onbruikbaar of ontoegankelijk zullen worden gemaakt of zullen worden gewist.
3. De bepalingen van het tweede en derde lid van artikel 312 zijn op dit misdrijf van toepassing.

## **Definitie DDoS**

De onderstaande definities zijn afkomstig uit het Cybersecurity Woordenboek, 2<sup>e</sup> druk (2019), tenzij anders wordt vermeld. *Toevoegingen en aanvullingen van CyberCrime Team Midden Nederland in cursief.*

### **Booter/Stresser**

Een dienst van criminelen om een DDoS-aanval mee uit te voeren. *Deze dienst wordt meestal tegen betaling aangeboden en maakt DDoS aanvallen mogelijk zonder veel technische kennis. Let op! Niet elke booter/stresser is crimineel: stress-testing diensten worden ook gebruikt om de beveiliging van systemen te testen.*

### **Bot**

Een computerprogramma dat zelfstandig taken kan uitvoeren. Bot is een afkorting van robot. Een bot kan onschuldig zijn, bijvoorbeeld als zoekmachines bots gebruiken om websites te vinden. Maar iemand kan een bot ook gebruiken om in te breken in een computer. Of om de computer zo klaar te maken dat een ander kan inbreken. Een computer die besmet is met een bot, noemt men ook wel een zombie. De gebruiker van een computer merkt vaak niets van een bot.

### **Botherder**

Iemand die een botnet beheert.

### **Botnet**

Een netwerk van computersystemen die zelfstandig kwaadaardige taken uitvoeren, zoals het versturen van spam of het uitvoeren van een DDoS-aanval. Een command-and-controlserver stuurt dit netwerk aan.

### **Command-and-controlserver**

Een machine die een aanvaller gebruikt om commando's te sturen naar systemen waarin hij heeft ingebroken. Bijvoorbeeld als hij een DDoS-aanval wil doen of een bot in een botnet wil aansturen.

**Cybercrime-as-a-service**

Een dienst van criminelen om tegen betaling een digitale aanval uit te voeren. Hun afnemers zijn vaak ook criminelen. Bekende voorbeelden zijn het stelen en doorverkopen van creditcardgegevens of medische gegevens, en kwaadaardige software of DDoS-aanvallen doorverkopen.

**DDoS**

Distributed Denial of Service.

Distributed Denial of Service is een vorm van Denial-of-Service waarbij een bepaalde dienst (bijvoorbeeld een website) niet beschikbaar wordt gemaakt door deze te bestoken met veel netwerkverkeer vanuit een groot aantal verschillende bronnen (Cybersecuritybeeld Nederland 2019).

**Denial of Service aanval**

Aanval waarbij men probeert om een computer, netwerk, of dienstverlening uit te schakelen voor de gewone gebruiker of klant. Zet men hiervoor meer computers in, dan gaat het om een Distributed Denial of Service (DDoS-aanval).

**DoS**

Denial of Service

**Scrubbing**

Gegevens filteren die naar een systeem gaan. Doel is onder andere om te zorgen dat DDoS-aanvallen niet succesvol kunnen zijn of om DDoS-aanvallen onschadelijk te maken. *Bekende oplossingen ter bescherming tegen DDoS zijn bijvoorbeeld NAWAS en Cloudflare.*