GEBRUIKSAANWIJZING

Bitdefender® CONSUMER SOLUTIONS

Digital Identity Protection

Bitdefender Digitale Identiteitsbescherming

Handleiding

Publicatiedatum 09/06/2023

Juridische kennisgeving

Bitdefender

Inhoudsopgave

OVER DEZE GIDS

Voor wie is deze handleiding bedoeld?

Deze gids is bedoeld voor alle Bitdefender gebruikers die Bitdefender Digital Identity Protection hebben gekozen als hun specifieke softwarehulpmiddel om zich te beschermen tegen de toenemende stroom van online gegevensinbreuken. De informatie in dit boek is niet alleen geschikt voor computergeletterden, maar is toegankelijk voor iedereen.

U zult ontdekken hoe u uw online privacy onder controle kunt krijgen door Bitdefender Digital Identity Protection het web te laten scannen op ongeoorloofde lekken van uw persoonlijke gegevens, te controleren of uw accounts zijn blootgesteld en het gemakkelijk te maken om actie te ondernemen ruim voordat er rampen toeslaan. U leert hoe u het beste uit Bitdefender kunt halen.

Wij wensen u veel aangenaam en nuttig leesplezier.

Hoe kunt u deze handleiding gebruiken?

De handleiding is ingedeeld aan de hand van enkele hoofdonderwerpen:

Aan de slag (pagina 6)

Kennismaking met Bitdefender Digital Identity Protection en de gebruikersinterface.

Datalekken (pagina 11)

Leer hoe u uw digitale identiteit goed kunt beschermen. Begin met te begrijpen wat datalekken zijn en hoe u ze kunt beoordelen om de juiste maatregelen te nemen voor de bescherming van uw online privacy.

Hulp vragen (pagina 17)

Informatie over waar u om hulp kunt vragen indien er zich onverwachte problemen voordoen.

Conventies die in deze gids worden gebruikt

Typografische conventies

In deze gids worden verschillende tekststijlen gebruikt, zodat de tekst leesbaarder is. De weergave en betekenis worden in de onderstaande tabel voorgesteld.

Weergave	Beschrijving
voorbeeld-syntaxis	Voorbeelden van syntaxis worden weergegeven in een niet-proportioneel lettertype.
https://www.bitdefender.com	De URL-koppeling wijst naar een externe locatie op http- of ftp-servers.
documentation@bitdefender.com	E-mailadressen worden in de tekst ingevoegd voor contactgegevens.
Over deze gids (pagina 1)	Dit is een interne koppeling naar een locatie in het document.
bestandsnaam	Namen van bestanden en mappen worden weergegeven in een niet-proportioneel lettertype.
optie	Alle productopties worden **vet** weergegeven.
trefwoord	Sleutelwoorden en belangrijke zinsdelen worden **vet** weergegeven.

Waarschuwingen

De waarschuwingen zijn grafisch gemarkeerde opmerkingen in de tekst die extra informatie over de huidige paragraaf onder de aandacht brengen.

Opmerking

De opmerking is slechts een kort commentaar. Hoewel u opmerkingen kunt weglaten, kunnen ze toch waardevolle informatie bieden zoals over een specifieke functie of een koppeling naar een verwant onderwerp.

Belangrijk

Dit vereist uw aandacht en het wordt niet aanbevolen dit te negeren. Doorgaans betreft het niet-kritieke, maar belangrijke informatie.

Waarschuwing

Dit is kritische informatie die u aandachtig moet lezen. Er zullen geen ernstige problemen optreden als u de aanwijzingen volgt. U moet de informatie lezen en begrijpen omdat hier iets wordt beschreven dat hoge risico's inhoudt.

Verzoek om commentaar

We willen u uitnodigen ons te helpen dit boek te verbeteren. Wij hebben alle informatie zo goed mogelijk getest en gecontroleerd. Laat ons weten of u enige tekortkomingen hebt ontdekt in dit boek of als u ideeën hebt om dit te verbeteren, zodat wij u de best mogelijke documentatie kunnen bieden.

U kunt contact met ons opnemen door een e-mail te sturen naar documentation@bitdefender.com. Wij verzoeken u al uw e-mails met betrekking tot de documentatie in het Engels te schrijven, zodat we uw opmerkingen op een efficiënte manier kunnen verwerken.

1. WAT IS BITDEFENDER DIGITAL IDENTITY PROTECTION

Online privacy en veiligheid zijn tegenwoordig enkele van de belangrijkste aandachtspunten voor internetgebruikers. En daar zijn goede redenen voor. Nu er steeds vaker grote datalekken plaatsvinden, is het absoluut noodzakelijk ervoor te zorgen dat uw persoonlijk identificeerbare informatie (PII) veilig is.

Maar wat kan worden geclassificeerd als persoonlijk identificeerbare informatie? Traditioneel werd gevoelige informatie zoals de volledige naam, het sofi-nummer, het rijbewijs, het postadres of creditcardgegevens als PII beschouwd. Uiteindelijk werd ook minder gevoelige informatie, zoals postcodes, IP-adressen of login-ID's, opgenomen. Na verloop van tijd kan uw digitale voetafdruk, dat wil zeggen de gegevens die u achterlaat als gevolg van uw surfen op het internet, een aantal van deze gegevens gaan omvatten.

Bitdefender Digital Identity Protection vertegenwoordigt de privéweg naar online vrijheid, waardoor u weer controle krijgt over uw digitale leven. En het vereist alleen uw naam, meest gebruikte e-mailadres en uw telefoonnummer. Op basis hiervan wordt zowel op het Surface Web als het Dark Web gezocht naar persoonlijke informatie die openbaar is gemaakt.

Bitdefender Digital Identity Protection biedt het volgende:

- **Monitoring- en detectiediensten:** het monitort meer dan 100 persoonlijk identificeerbare informatie-items zoals sofi-nummers, creditcards of huisadres, en toont alle gevonden gegevens over uw online voetafdruk.

  > **Opmerking**
  > Bitdefender bewaart of verwerkt geen persoonlijk identificeerbare informatie. Alleen verwijzingen naar mogelijke datalekken worden bijgehouden, zonder gevoelige gegevens.

- **Real time waarschuwingen:** U ontvangt meldingen over datalekken en blootgestelde gegevens in Dark Web, persoonlijke informatie in Surface Web en potentiële imitators op sociale media.
- **Oplossingen:** Onze service stelt duidelijke acties voor die nodig zijn om problemen op te lossen en stuurt herinneringen als een probleem

niet volledig is opgelost. Er kunnen ook instructies gegeven worden over hoe u de gepersonaliseerde advertenties kunt verwijderen, uw gegevens kunt exporteren of de tracking kunt uitschakelen.

2. AAN DE SLAG

2.1. Activeer Digitale Identiteitsbescherming

Activeer het Bitdefender Digital Identity Protection-abonnement nadat uw bestelling is geplaatst en betaald.

1. Open de bevestigingsmail die u kort na het afronden van uw bestelling ontvangt en klik op **AAN DE SLAG**.
2. U wordt doorgestuurd naar https://central.bitdefender.com.
   Meld u aan met uw Bitdefender Central-account. Als u geen account hebt, kunt u er een aanmaken.
3. Na aanmelding wordt het abonnement automatisch gekoppeld aan uw Central-account en start het onboardingproces.

U kunt ook:

- ga naar het **Mijn Abonnementen** paneel vanuit Central, aan de linkerkant van het venster, en klik op **+ Activeren met code**.
- voer de 10-cijferige sleutel in die u in uw bevestigingsmail hebt gevonden en druk op **ACTIVEREN**.
- selecteer, indien gevraagd, hoe u de code wilt gebruiken en klik dan op **ACTIVEREN**.

2.2. Configureer Digitale Identiteitsbescherming

1. Ga naar https://central.bitdefender.com/ en log in op uw account.
   Als u nog geen account hebt, klik dan op **CREËER ACCOUNT**, typ uw volledige naam, een e-mailadres en een wachtwoord.
2. Selecteer het Digital Identity Protection-paneel.
   Er verschijnt een welkomstscherm.
3. Klik op **BEGINNEN**.
4. U wordt nu geïnformeerd over welke informatie u moet verstrekken. Uw gegevens worden altijd versleuteld en beveiligd.
   Klik op **VOLGENDE**.
5. Typ uw voornaam, tweede voornaam (indien van toepassing) en achternaam in de overeenkomstige vakken en klik dan op **VOLGENDE**.

6. Voer uw e-mailadres in en klik op **VOLGENDE**.
   Zorg ervoor dat het een geldig e-mailadres is waartoe u toegang hebt.
7. Er wordt een beveiligingscode naar het door u opgegeven adres gestuurd.
   Open uw e-mail, kopieer de code en plak deze in het overeenstemmende veld.
   Klik daarna op **CONTROLEREN**.
8. Selecteer uw land en voer uw telefoonnummer in, en klik vervolgens op **VOLGENDE**.
9. U zou kort daarna een beveiligingscode moeten ontvangen.
   Voer de code in en selecteer **CONTROLEREN**.
10. Nadat de eerste controle is uitgevoerd, klikt u op **VOLTOOIEN**.

.

> **Opmerking**
> U wordt geïnformeerd indien bij deze eerste controle inbreuken, persoonlijk identificeerbare informatie of mogelijke pogingen tot imitatie worden ontdekt.

Bitdefender Digital Identity Protection is nu geconfigureerd.

2.3. Bekijk uw digitale voetafdruk, inbreuken op gegevens en mogelijke imitaties

Nadat u de configuratie hebt voltooid, voert Bitdefender Digital Identity Protection een online controle uit om mogelijke imitaties, datalekken en persoonlijk identificeerbare informatie op het Open Web te ontdekken. Wij raden u aan om alle informatie in de tabbladen **DIGITALE VOETAFDRUK**, **DATALEKKEN** en **IMITATIECONTROLE** te bekijken.

- Uw Digitale Voetafdruk evalueren (pagina 10)
- Datalekken evalueren (pagina 11)
- Evalueren van mogelijke imitaties (pagina 12)

2.4. Verbeter de controle

We gebruiken de gegevens die u voorziet om het Surface Web en het Dark Web te monitoren en enige activiteiten te detecteren die uw privacy of uw persoonlijke reputatie zouden kunnen aantasten.

Als u een ander e-mailadres of een ander telefoonnummer wilt toevoegen, klik dan op ⊕, klik dan op **E-MAILADRES TOEVOEGEN** of **TELEFOONNUMMER TOEVOEGEN** en volg de instructies.

3. DASHBOARD

Het Dashboard voegt informatie samen uit de secties **DIGITALE VOETAFDRUK**, **DATALEKKEN** en **IMITATIECONTROLE**.

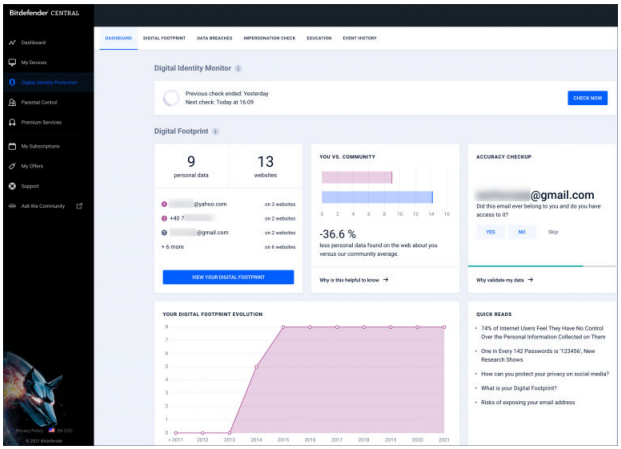
Dit omvat het volgende:

- Uw blootgestelde gegevens en hun webbronnen
- De gemiddelde hoeveelheid blootgestelde gegevens voor de hele gemeenschap
- De evolutie van uw digitale voetafdruk
- Inhoud met betrekking tot privacy
- Gegevensinbreuken
- Het gemiddelde aantal datalekken binnen de gemeenschap

3.1. Digital Identity Monitor

Het systeem van Bitdefender zoekt, aan de hand van nauwkeurige informatie, naar persoonsgegevens die zijn blootgesteld op het Open Web en het Dark Web, en scant alle voornaamste sociale mediaplatformen op zoek naar aanwijzingen van pogingen tot imitatie.

Klik op **NU CONTROLEREN** om een online scan uit te voeren.



4. DIGITALE VOETAFDRUK

Uw persoonlijk identificeerbare informatie en hun bronnen verschijnen hier. Het is aan u om te beoordelen of het openbaar maken van de informatie op het web een bedreiging vormt.

Onze AI-gestuurde monitor is sterk afhankelijk van correcte gegevens om nieuwe dreigingen te detecteren, dus laat ons weten of de informatie juist of onjuist is.

Zodra u bevestigt dat bepaalde informatie van u is, voegen wij deze toe aan ons monitoringsysteem en vergroten wij de kans om in de toekomst andere informatie te ontdekken.

4.1. Uw Digitale Voetafdruk evalueren

Om uw digitale voetafdruk te evalueren:

1. Ga naar het tabblad **DIGITALE VOETAFDRUK**.
2. Informatie die nog niet geverifieerd is, verschijnt met de tekst **Verifiëren** aan de rechterkant. Klik op **Verifiëren** en selecteer vervolgens Ja of Nee, afhankelijk van het geval.

> **Opmerking**
> Elk bevestigd informatie-item wordt toegevoegd aan ons monitoringalgoritme, waardoor de door onze diensten getoonde resultaten verbeteren. Informatie die wordt afgewezen, wordt niet langer weergegeven. Ze blijft echter wel beschikbaar op het web.

5. DATALEKKEN

Lekken doen zich voor wanneer hackers erin slagen de beveiligingsmaatregelen van een bedrijf te omzeilen en uw persoonlijke informatie te bemachtigen, om die vervolgens te verkopen op het Dark Web. Cybercriminelen richten zich meestal op inloggegevens, persoonlijk identificeerbare informatie (PII), medische gegevens en bankgegevens.

Elke organisatie of dienst kan het slachtoffer worden van een datalek, maar organisaties met een groot klantenbestand zijn een aantrekkelijker doelwit. Inbreuken omvatten gewoonlijk namen, e-mailadressen, gebruikersnamen, wachtwoorden, postadressen, telefoonnummers, sofi-nummers en creditcardgegevens (nummer, vervaldatum, CVV).

5.1. Datalekken evalueren

Om uw datalekken te evalueren:

1. Ga naar het tabblad **DATALEKKEN**.
2. Onder sommige items vindt u een lijst met acties die nodig zijn om uw account te beveiligen. Na het uitvoeren van een actie klikt u op het vakje ernaast om te bevestigen.
   Als u niet zeker weet hoe u een taak moet uitvoeren, kunt u altijd op de link in de taakbeschrijving klikken en wordt u doorgestuurd naar een pagina waar u alle nodige stappen vindt.
   Niet alle inbreuken kunnen op deze manier worden aangepakt. Sommige, zoals **Collection #1**, bevatten geen stappen. In plaats daarvan wordt u doorverwezen naar online beschikbare artikels waar u meer hulp kunt vinden.

   Opmerking
   Bitdefender bewaart of verwerkt geen persoonlijk identificeerbare informatie. Alleen verwijzingen naar mogelijke datalekken worden bewaard, zonder gevoelige gegevens op te nemen.

6. CONTROLE IMITATIES

Criminelen die bekend staan als "pretexters" maken op allerlei manieren gebruik van de kunst van het zich voordoen als een vertrouwd persoon om hun slachtoffers te misleiden en toegang te krijgen tot gevoelige informatie. "Pretexting" wordt gedefinieerd als het zich voordoen als iemand anders om een ontvanger te manipuleren tot het verstrekken van gevoelige gegevens zoals wachtwoorden, creditcardnummers of andere vertrouwelijke informatie.

Bitdefender Digital Identity Protection bewaakt 25 sociale mediaplatformen en brengt u onmiddellijk op de hoogte als een profiel wordt gevonden dat een poging tot imitatie zou kunnen zijn.

6.1. Evalueren van mogelijke imitaties

In het tabblad **IMITATIECONTROLE** worden alle mogelijke pogingen weergegeven. Voor elke detectie kunt u een van drie mogelijkheden kiezen:

- Het is een poging tot imitatie
- Het is uw eigen profiel
- Het is een ander profiel

Afhankelijk van de Bitdefender Digital Identity Protectionkeuze zal specifieke stappen aanbevelen om het probleem aan te pakken. Telkens wanneer u een stap hebt voltooid, kunt u deze markeren als **Gereed**.

7. OPLEIDING

Het tabblad Opleiding dient als kennisbank waar gebruikers meer informatie kunnen vinden over hoe zij hun digitale identiteit kunnen beschermen.

De hier vermelde artikels kunnen in verschillende categorieën worden ingedeeld:

- Lekken
- Blootstellingen
- Nabootsing van identiteit

Voor toegang tot de volledige versie van een artikel, klikt u op de overeenstemmende **Meer informatie** link.

8. EVENTGESCHIEDENIS

De sectie Gebeurtenishistorie is het middel waarmee wij voortdurend met onze gebruikers communiceren. Het is een chronologisch geordende lijst van gebeurtenissen met betrekking tot de bescherming van uw Digitale Identiteit.

Naast nieuw gedetecteerde dreigingen (indien aanwezig), kunt u terugkeren naar deze pagina voor waardevol advies over hoe u zich online correct kunt gedragen, om de kans te vergroten dat u niet te maken krijgt met privacyproblemen.

In de sectie Gebeurtenishistorie vindt u de volgende informatie:

- Uitgevoerde acties
- Service-updates
- Datalekken

9. VEELGESTELDE VRAGEN

Waarom is online privacy tegenwoordig zo belangrijk?

Online privacy betekent het beschermen van uw privé- en financiële gegevens tegen cybercriminelen. Dergelijke persoonlijk identificeerbare informatie heeft grote waarde op het internet en zodra deze gegevens uitlekken, is uw geld niet langer veilig. U hebt een betrouwbare dienst nodig voor continue identiteitsbescherming en -bewaking om ervoor te zorgen dat uw privégegevens altijd privé blijven.

Wat is mijn digitale voetafdruk?

Uw digitale voetafdruk is uw gehele online activiteit. Elke login op uw sociale accounts, elke banktransactie, alles wat u online koopt kan worden blootgesteld aan datalekken. U moet zich te allen tijde bewust zijn van de manier waarop uw persoonlijke en financiële gegevens worden opgeslagen en behandeld - en de nodige stappen ondernemen om ze te beschermen.

Wat zijn datalekken en hoe beïnvloeden ze mijn persoonlijke accounts?

Datalekken zijn beveiligingsincidenten waarbij privégegevens uitlekken naar een onveilige omgeving. Deze kunnen door cybercriminelen overal ter wereld worden misbruikt om toegang te krijgen tot uw online identiteit. Datalekken kunnen gevolgen hebben voor uw kredietscore, ziekteverzekering, studiebeurzen of zelfs uw pensioenrekening.

Hoe kan Bitdefender Digital Identity Protection helpen met mijn online privacy?

Bitdefender Digital Identity Protection bewaakt voortdurend uw persoonlijke gegevens en waarschuwt u in real time in geval van een datalek. Zo kunt u uw wachtwoorden wijzigen en uw accounts beveiligen om financieel verlies of imitaties op sociale media te voorkomen.

Waar zoekt Bitdefender Digital Identity Protection naar gegevens?

Bitdefender Digital Identity Protection zoekt naar gegevens op het Surface Web (sociale medianetwerken, berichten, blogs, forums, gegevensmakelaars, publicaties, offline databases) maar ook op de Dark Web-marktplaatsen, waar cybercriminelen informatie verhandelen die is verzameld uit datalekken.

Hoe verschilt Bitdefender Digital Identity Protection van andere (gratis) diensten?

Bitdefender Digital Identity Protection heeft ongeëvenaarde mogelijkheden om aanzienlijke volumes en een hogere kwaliteit van gegevens van het Dark Web te bewaken. De informatie van het Dark Web wordt gecureerd en ontdubbeld zodat we het aantal vals-positieve waarschuwingen kunnen verminderen.

Hoe kan ik de dienst gebruiken? Moet ik iets downloaden?

U hoeft niets te downloaden, want Bitdefender Digital Identity Protection is een online dienst. U krijgt toegang tot een web-dashboard waar u al uw persoonlijke accounts in real time kunt controleren.

Hoe kan ik waarschuwingen ontvangen voor toekomstige datalekken?

Om waarschuwingen te ontvangen voor toekomstige datalekken hoeft u zich alleen maar aan te melden voor e-mailwaarschuwingen vanuit uw web-dashboard, en u begint privacywaarschuwingen en beveiligingsrapporten te ontvangen van Bitdefender Digital Identity Protection.

10. HULP VRAGEN

10.1. Hulp vragen

Bitdefender biedt zijn klanten een ongeëvenaard niveau van snelle en nauwkeurige ondersteuning. Als u een probleem ondervindt of een vraag hebt over uw Bitdefender-product, kunt u verschillende online bronnen gebruiken om een oplossing of een antwoord te vinden. Tegelijkertijd kunt u contact opnemen met het klantenserviceteam van Bitdefender. Onze ondersteuningsmedewerkers zullen uw vragen tijdig beantwoorden en u de hulp bieden die u nodig hebt.

10.2. Online bronnen

Er zijn meerdere online informatiebronnen beschikbaar om u te helpen bij het oplossen van problemen en vragen met betrekking tot Bitdefender.

- Bitdefender Support Center:
  https://www.bitdefender.nl/consumer/support/
- De Community van Bitdefender-experts:
  https://community.bitdefender.com/en/
- Bitdefender Cyberpedia:
  https://www.bitdefender.com/cyberpedia/

U kunt ook uw favoriete zoekmachine gebruiken om meer informatie te zoeken over computerbeveiliging, de Bitdefender-producten en het bedrijf.

10.2.1. Bitdefender Support Center

Het Bitdefender Support Center is een online opslagplaats van informatie over Bitdefender-producten. Hier worden rapporten bijgehouden in een gemakkelijk toegankelijk formaat over de doorlopende technische ondersteuning en activiteiten voor foutoplossingen van de ondersteunings- en ontwikkelingsteams van Bitdefender. Daarnaast vindt u hier ook meer algemene artikels over dreigingspreventie, het beheer van Bitdefender-oplossingen met gedetailleerde uitleg en talrijke andere artikels.

De Bitdefender Support Center is toegankelijk voor het publiek en kan vrij worden doorzocht. De uitgebreide informatie die de database bevat is nog

een middel om BitDefender-klanten de technische kennis en het inzicht te bieden die ze nodig hebben. Alle geldige aanvragen voor informatie of foutrapporten die van BitDefender-klanten komen, vinden uiteindelijk hun weg naar de Bitdefender Support Center als rapporten over het oplossen van problemen, tips om een probleem te omzeilen of informatieve artikels om de helpbestanden van het product aan te vullen.

Het Bitdefender Support Center is te allen tijde beschikbaar op het volgende adres: https://www.bitdefender.nl/consumer/support/.

10.2.2. De Community van Bitdefender-experts

De Community van Experts is een omgeving waar gebruikers, enthousiastelingen en fans van Bitdefender aan kunnen deelnemen, waar ze ideeën kunnen uitwisselen, elkaar kunnen ondersteunen en hun kennis en oplossingen kunnen delen. Het is ook een plaats voor brainstorming en een bron van waardevolle feedback aan onze ontwikkelingsteams. De leden van de gemeenschap zijn ervaren Bitdefender-gebruikers die in hun eigen tijd graag anderen helpen. Met hun enorme bijdrage en oprechte vrijwillige inspanningen hebben we een kennisbank gecreëerd waar gebruikers antwoorden en begeleiding kunnen vinden, maar met dat menselijke tintje.

Hier vindt u zinvolle gesprekken met mensen die Bitdefender gebruiken op hun apparaten. De gemeenschap biedt een echte band met onze leden en laat uw stem horen. Het is een plek waar u wordt aangemoedigd om deel te nemen in de wetenschap dat uw mening en inbreng worden gerespecteerd en gekoesterd. Als gewaardeerde provider streven we ernaar een ongeëvenaard niveau van snelle, accurate ondersteuning te bieden en willen we onze gebruikers dichter bij ons brengen. Wij hebben onze gemeenschap met dit doel voor ogen ontworpen.

U vindt de website van onze Community van experts hier:

https://community.bitdefender.com/en/

10.2.3. Bitdefender Cyberpedia

Bitdefender Cyberpedia heeft alle informatie die u nodig hebt over de nieuwste cyberdreigingen. Dit is de plaats waar Bitdefender-experts tips en trucs delen over hoe u beschermd kunt blijven tegen hackers, datalekken, identiteitsdiefstal en pogingen tot sociale imitatie.

De webpagina van Bitdefender Cyberpedia vindt u hier:

https://www.bitdefender.com/cyberpedia/.

10.3. Contactinformatie

Efficiënte communicatie is de sleutel tot succes. Sinds 2001 heeft BITDEFENDER een onberispelijke reputatie opgebouwd door voortdurend te streven naar een betere communicatie om de verwachtingen van onze klanten en partners telkens te overtreffen. Aarzel daarom niet om rechtstreeks contact met ons op te nemen als u iets wilt vragen, via onze Bitdefender Support Center.

https://www.bitdefender.nl/consumer/support/

10.3.1. Lokale verdelers

De lokale BitDefender-verdelers zijn altijd paraat om te reageren op aanvragen met betrekking tot hun bedrijfsgebied, zowel op commercieel als algemeen vlak.

Om een Bitdefender-verdeler te vinden in uw land:

1. Ga naar https://www.bitdefender.com/partners/partner-locator.html.
2. Kies uw land en stad met de overeenkomstige opties.

WOORDENLIJST

Activeringscode

Is een unieke sleutel die u in de handel kunt kopen en die gebruikt wordt om een specifiek product of een dienst te activeren. Met een activeringscode kan een geldig abonnement voor een bepaalde periode en een bepaald aantal toestellen geactiveerd worden en kunt u ook gebruiken om het abonnement te verlengen, op voorwaarde dat het voor hetzelfde product of dezelfde dienst is.

ActiveX

ActiveX is een model voor het schrijven van programma's zodat andere programma's en het besturingssysteem ze kunnen oproepen. De ActiveX-technologie wordt gebruikt bij Microsoft Internet Explorer om interactieve Webpagina's te maken die eruitzien en zich gedragen als computerprogramma's in plaats van statische pagina's. Met ActiveX kunnen gebruikers vragen stellen of beantwoorden, drukknoppen gebruiken en op andere manieren interactief omgaan met de Webpagina. ActiveX-besturingselementen zijn vaak geschreven met de hulp van Visual Basic. ActiveX is berucht door een compleet gebrek aan beveiligingscontroles; computerbeveiligingsexperts raden het gebruik ervan via het internet sterk af.

Advanced persistent threat

Geavanceerde aanhoudende dreiging (Advanced Persistent Threat - APT) maakt misbruik van kwetsbare plekken in systemen om belangrijke informatie te stelen en aan de bron te leveren. Grote groepen, zoals organisaties, bedrijven of overheden zijn doelgroepen voor deze bedreiging. Het doel van een advanced persistent threat is heel lang onopgemerkt te blijven en belangrijke informatie in te kijken en te verzamelen, zonder de toestellen te beschadigen. De methode die gebruikt wordt om de bedreiging in het netwerk te brengen verloopt via een pdf-bestand of een Office-document dat er onschuldig uitziet, zoadat elke gebruiker de bestanden kan openen.

Adware

Adware wordt vaak gecombineerd met een hosttoepassing die gratis wordt aangeboden op voorwaarde dat de gebruiker akkoord gaat met het uitvoeren van de adware. Omdat adware-toepassingen doorgaans

worden geïnstalleerd nadat de gebruiker een licentieovereenkomst die het doel van de toepassing vermeldt heeft geaccepteerd, wordt er geen inbreuk gepleegd. Pop-upadvertenties kunnen echter irritant worden en in sommige gevallen de systeemprestaties negatief beïnvloeden. De gegevens die door sommige van deze toepassingen worden verzameld, kunnen bovendien privacy-problemen veroorzaken voor gebruikers die niet volledig op de hoogte waren van de voorwaarden van de licentieovereenkomst.

Archive

Een schijf, tape, of map die bestanden bevat waarvan een back-up werd gemaakt.

Een bestand dat één of meer bestanden bevat in een gecomprimeerd formaat.

Backdoor

Een gat in de beveiliging van een systeem, dat opzettelijk werd achtergelaten door ontwikkelaars of beheerders. De motivatie voor dergelijke gaten is niet altijd boosaardig. Sommige besturingssystemen worden bijvoorbeeld geleverd met bevoegde accounts die bedoeld zijn voor gebruik door technici voor service ter plaatse of onderhoudsprogrammeurs van de leverancier.

Boot sector

Een sector aan het begin van elke schijf die de architectuur van de schijf identificeert (sectorgrootte, clustergrootte, enz.) Bij opstartschijven bevat de opstartsector ook een programma dat het besturingssysteem laadt.

Boot virus

Een bedreiging die de opstartsector van een vaste schijf of een diskette infecteert. Wanneer u probeert op te starten vanaf een diskette die geïnfecteerd is met een opstartsectorvirus, zal de bedreiging actief worden in het geheugen. Wanneer u vanaf dat ogenblik uw systeem opstart, zal de bedreigingen telkens in het geheugen geactiveerd zijn.

Botnet

Het woord "botnet" is samengesteld uit de woorden "robot" en "netwerk". Botnets zijn apparaten die met het internet verbonden zijn en met bedreigingen geïnfecteerd zijn en kunnen gebruikt worden om spammail te verzenden, data te stelen, kwetsbare apparaten van op afstand

te controleren of om spyware, ransomware en andere schadelijke bedreigingen te verspreiden. Het doel ervan is zoveel mogelijk apparaten te infecteren, bijvoorbeeld pc's, servers, mobiele of IoT-apparaten die eigendom zijn van grote bedrijven of sectoren.

Browser

De korte naam voor Webbrowser, een softwaretoepassing die wordt gebruikt op Webpagina's te zoeken en weer te geven. Populaire browsers omvatten Microsoft Internet Explorer, Mozilla Firefox en Google Chrome. Dit zijn grafische browsers. Dit betekent dat ze zowel grafische beelden als tekst kunnen weergeven. Bovendien kunnen de meeste moderne browsers ook multimedia-informatie voorstellen met geluid en video, hoewel voor sommige formaten plug-ins vereist zijn.

Brute Force-aanval

Aanval via raden van wachtwoord, gebruikt om in te breken in een computersysteem door mogelijke wachtwoordcombinaties in te geven, meestal te beginnen met het meest eenvoudig te raden wachtwoord.

Opdrachtregel

In een opdrachtregelinterface typt de gebruiker opdrachten in opdrachttaal rechtstreeks op het scherm in de ruimte die hiervoor wordt geboden.

Cookies

Binnen de Internetindustrie worden cookies beschreven als kleine programma's die informatie bevatten over individuele computers, die door adverteerders wordt geanalyseerd en gebruikt om uw on line interesse en smaak te volgen. De cookietechnologie wordt in dit kader nog steeds verder ontwikkeld met het doel reclameberichten rechtstreeks te richten op de interesses die u hebt meegedeeld. Dit is voor veel mensen een mes dat aan twee kanten snijdt. Aan de ene kant is het efficiënt en relevant aangezien u alleen reclames ontvangt voor zaken waarvoor u interesse hebt. Aan de andere kant betekent het ook dat elke plaats die u bezoekt en alles wat u aanklikt wordt "opgespoord" en "gevolgd". Het is dan ook te begrijpen dat er heel wat wordt gedebatteerd over privacy. Bovendien zijn veel mensen verontwaardigd omdat ze het gevoel hebben dat ze als een "SKU-nummer" worden beschouwd (u weet wel, de barcode op de verpakkingen die bij de kassa van het warenhuis wordt gescand). Hoewel dit standpunt misschien nogal extreem is, is het vaak een bijzonder nauwkeurige omschrijving.

Cyberpesten

Wanneer collega's of onbekenden met opzet onrechtmatige daden stellen tegenover kinderen, met de bedoeling om fysiek te kwetsen. Om emotionele schade te berokkenen, sturen de daders gemene berichten of onflatteuze foto's om hun slachtoffers af te zonderen van anderen of gefrustreerd te doen voelen.

Woordenboekaanval

Aanval via raden van wachtwoord, gebruikt om in te breken in een computersysteem door een combinatie van veel voorkomende woorden in te geven om zo mogelijke wachtwoorden te genereren. Dezelfde methode wordt gebruikt om decryptiesleutels van versleutelde berichten of documenten te raden. Woordenboekaanvallen slagen in hun opzet omdat veel mensen korte wachtwoorden gebruiken die uit slechts één woord bestaan en die makkelijk te raden zijn.

Schijfstation

Dit is een apparaat dat gegevens leest van en schrijft naar een schijf. Een harde-schijfstation leest en schrijft harde schijven. Een diskettestation opent diskettes. Schijfstations kunnen intern (binnen de behuizing van een computer) of extern zijn (in een afzonderlijke behuizing die op de computer wordt aangesloten).

Download

Om gegevens (meestal een volledig bestand) te kopiëren van een hoofdbron naar een randapparaat. De term wordt vaak gebruikt om het proces te beschrijven waarbij een bestand van een on line-service wordt gekopieerd naar de eigen computer. Downloaden kan ook verwijzen naar het kopiëren van een bestand van een netwerkbestandsserver naar een computer in het netwerk.

E-mail

Elektronische post. Een dienst die berichten naar computers verzendt via lokale of globale netwerken.

Gebeurtenissen

Een actie of gebeurtenis die door een programma wordt gedetecteerd. Gebeurtenissen kunnen gebruikersacties zijn, zoals het klikken met de muis of het indrukken van een toets, of systeemgebeurtenissen, zoals een tekort aan geheugen.

Exploits

Een manier om misbruik te maken van verschillende bugs of kwetsbaarheden in een computer (software of hardware). Zo kunnen hackers de controle over computers of over netwerken in handen krijgen.

Vals positief

Doet zich voor wanneer een scanner een bestand ten onrechte beschouwt als geïnfecteerd.

Bestandsextensie

Het gedeelte van een bestandsnaam achter de punt, waarmee het gegevenstype dat in het bestand is opgeslagen wordt aangeduid. Heel wat besturingssystemen, zoals Unix, VMS en MS-DOS, maken gebruik van bestandsextensies. Ze gebruiken doorgaans één tot drie letters (sommige betreurenswaardige oude besturingssystemen ondersteunen niet meer dan drie letters). Voorbeelden hiervan zijn "c" voor C-broncode, "ps" voor PostScript, "txt" voor tekst zonder opmaak.

Heuristisch

Een methode voor het identificeren van nieuwe bedreigingen op basis van regels. Deze scanmethode is niet gebaseerd op een specifieke informatie-database voor bedreigingen. Het voordeel van de heuristische scan is dat hij zich niet laat misleiden door een nieuwe variant van een bestaande bedreiging. Dit type kan echter af en toe een verdachte code rapporteren in normale programma's, zodat de zogenoemde "valse positieve" rapporten worden gegenereerd.

Honeypot

Een afleiding in uw computersysteem dat hackers aantrekt om te onderzoeken hoe ze te werk gaan en de afwijkende methodes die ze gebruiken om systeeminformatie te verzamelen, te identificeren. Bedrijven zijn steeds meer geïnteresseerd om honingpotten te implementeren en te gebruiken om hun algemene beveiligingsstatus te verbeteren.

IP

Internet Protocol - Een routeerbaar protocol in de TCP/OP-protocolreeks die verantwoordelijk is voor de IP-adressering, routing en de fragmentatie en defragmentatie van IP-pakketten.

Java applet

Een Java-programma dat is ontwikkeld om alleen op een webpagina te worden uitgevoerd. Om een applet op een webpagina te gebruiken, zou u de naam van het applet opgeven en de grootte (lengte en breedte in pixels) die het applet kan gebruiken. Wanneer de webpagina wordt geopend, downloadt de browser het applet van een server en voert hij het uit op de computer van de gebruiker (de client). Applets onderscheiden zich van toepassingen omdat ze worden beheerd door een streng beveiligingsprotocol.

Zelfs wanneer applets op de client worden uitgevoerd kunnen ze, bijvoorbeeld, geen gegevens lezen van of schrijven naar de computer van de client. Bovendien worden applets verder beperkt zodat ze alleen gegevens kunnen lezen van en schrijven naar hetzelfde domein waarvan ze worden bediend.

Keylogger

Een keylogger is een toepassing die alles wat u typt, logt. Keyloggers zijn in wezen niet kwaadaardig. Ze kunnen worden gebruikt voor rechtmatige doeleinden, zoals het bewaken van de activiteiten van werknemers of kinderen. Ze worden echter steeds meer gebruikt door cybercriminele voor boosaardige doeleinden (bijv. voor het verzamelen van persoonlijke gegevens, zoals aanmeldingsgegevens en nummer van de sociale zekerheid).

Macro virus

Een type computerbedreiging die is gecodeerd als een macro die in een document is ingesloten. Talrijke toepassingen, zoals Microsoft Word en Excel, ondersteunen krachtige macrotalen. Met deze toepassingen kan u een macro in een document insluiten, en die macro telkens laten uitvoeren wanneer het document wordt geopend.

Mail client

Een e-mailclient is een toepassing waarmee u e-mail kunt verzenden en ontvangen.

Geheugen

Interne opslaggebieden in de computer. De term geheugen staat voor gegevensopslag die in de vorm van chips wordt geleverd. Het woord opslag wordt gebruikt voor geheugen dat aanwezig is op tapes of schijven. Elke computer wordt geleverd met een bepaalde hoeveelheid fysiek geheugen, dat meestal het hoofdgeheugen of RAM wordt genoemd.

Niet-heuristisch

Deze scanmethode is gebaseerd op een specifieke informatie-database voor bedreigingen. Het voordeel van de niet-heuristische scan is dat deze zich niet laat misleiden door iets dat kan lijken op een bedreiging en geen vals alarm genereert.

Online predatoren

Personen die minderjarigen of adolescenten met opzet willen betrekken in gesprekken, om hen zo te betrekken in illegale seksuele activiteiten. Sociale netwerken zijn de ideale plaats waar kwetsbare kinderen gemakkelijk kunnen worden verleid om seksuele activiteiten uit te voeren, online of tijdens fysieke ontmoetingen.

Ingepakte programma's

Een bestand in een gecomprimeerd formaat. Talrijke besturingssystemen en toepassingen beschikken over opdrachten waarmee u bestanden kunt inpakken, zodat ze minder geheugen in beslag nemen. Veronderstel bijvoorbeeld dat u een tekstbestand hebt dat tien opeenvolgende spatietekens bevat. Normaal zou dit tien bytes opslagruimte vereisen.

Een programma dat bestanden inpakt kan echter de spatietekens vervangen door een speciaal spatiereeks-teken, gevolgd door het aantal spaties dat wordt vervangen. In dit geval hebben de tien spaties slechts twee bytes nodig. Dit is slechts één inpaktechniek, maar er zijn er veel meer.

Pad

De exacte weg naar een bestand op een computer. Deze weg wordt doorgaans beschreven door middel van het hiërarchische bestandssysteem van boven naar beneden.

De route tussen twee willekeurige punten, zoals het communicatiekanaal tussen twee computers.

Phishing

Het onder valse voorwendselen verzenden van een e-mail aan een gebruiker, waarbij de indruk wordt gewekt dat het bericht afkomstig is van een bestaande onderneming, in een poging de gebruiker persoonlijke gegevens te ontfutselen die zullen worden gebruikt voor identiteitsroof. In het e-mailbericht wordt de gebruiker doorverwezen naar een website waar persoonlijke gegevens kunnen worden bijgewerkt,

zoals wachtwoorden en creditcard-, sofi- en bankrekeningnummers, die reeds in het bezit zijn van de rechtmatige organisatie. De website is echter nep en alleen opgezet om de gebruikersgegevens te stelen.

Foton

Photon is een vernieuwende, niet opdringerige Bitdefender technologie, ontworpen om de invloed van uw beveiligingsoplossing op de prestaties te beperken. Door de activiteit van uw pc's op de achtergrond te bewaken, maakt het gebruikspatronen die helpen opstart- en scanprocessen te optimaliseren.

Polymorf virus

Een bedreiging die zijn vorm wijzigt bij elk bestand dat het infecteert. Aangezien ze geen consequent binair patroon hebben, zijn dergelijke bedreigingen moeilijk te identificeren.

Poort

Een interface op een computer waarop u een apparaat kan aansluiten. PC’s hebben verschillende types poorten. Intern zijn er verschillende poorten voor het aansluiten van schijfstations, beeldschermen en toetsenborden. Extern beschikken PC’s over poorten voor het aansluiten van modems, printers, muizen en andere randapparatuur.

Bij TCP/IP- en UDP-netwerken, zijn ze een eindpunt voor een logische verbinding. Het poortnummer duidt aan over welk type poort het gaat. Poort 80 wordt bijvoorbeeld gebruikt voor HTTP-verkeer.

Ransomware

Ransomware is kwaadaardige software waarmee criminelen proberen geld af te persen van gebruikers, door hun systemen ontoegankelijk te maken totdat er losgeld is betaald. Enkele van de vele varianten van ransomware voor persoonlijke computersystemen zijn CryptoLocker, CryptoWall en TeslaWall.

De infectie kan verspreid worden door spam-e-mail te openen, e-mailbijlagen te openen of toepassingen te installeren zonder dat de gebruiker weet wat er op zijn systeem gaande is. Dagelijkse gebruikers en bedrijven vormen een doelwit voor ransomwarehackers.

Rapportbestand

Een bestand dat de acties weergeeft die zich hebben voorgedaan. BitDefender houdt een rapportbestand bij met het gescande pad,

het aantal gescande mappen, archieven en bestanden, en het aantal gevonden geïnfecteerde en verdachte bestanden.

Rootkit

Een rootkit is een verzameling softwareprogramma's die op beheerdersniveau toegang biedt tot een systeem. Deze term werd voor het eerst gebruikt voor Unix-besturingssystemen en verwees naar opnieuw gecompileerde hulpprogramma's die beheerdersrechten gaven aan indringers, zodat ze hun aanwezigheid konden verbergen en onzichtbaar bleven voor de echte systeembeheerders.

De belangrijkste functie van rootkits is het verbergen van processen, bestanden, logins en logbestanden. Rootkits die de hiervoor benodigde software bevatten, kunnen ook gegevens onderscheppen van terminals, netwerkverbindingen of randapparaten.

Rootkits zijn in wezen niet kwaadaardig. Systemen en zelfs sommige toepassingen verbergen kritieke bestanden met de hulp van rootkits. Ze worden echter het vaakst gebruikt om bedreigingen of de aanwezigheid van een indringer op het systeem te verbergen. In combinatie met bedreigingen, vormen rootkits een ernstige bedreiging voor de integriteit en beveiliging van een systeem. Ze kunnen het verkeer controleren, achterpoortjes in het systeem maken, bestanden en logboeken wijzigen en detectie vermijden.

Script

Script, een andere term voor een macro of batchbestand, is een lijst opdrachten die kunnen worden uitgevoerd zonder tussenkomst van de gebruiker.

Spam

Elektronische junkmail of berichten van junknieuwsgroepen. Algemeen bekend als ongewenste e-mail.

Spyware

Elke software die heimelijk gebruikersgegevens verzamelt via de internetverbinding van de gebruikers zonder dat hij/zij zich hiervan bewust is, doorgaans voor reclamedoeleinden. Spywaretoepassingen worden doorgaans gebundeld als een verborgen onderdeel van freeware- of sharewareprogramma's die kunnen worden gedownload van het internet. We moeten echter wel vermelden dat de meeste shareware- en freewaretoepassingen geen spyware bevatten. Zodra de spyware is

geïnstalleerd, worden de activiteiten van de gebruiker op het internet gevolgd en wordt deze informatie op de achtergrond naar iemand anders doorgestuurd. Spyware kan ook informatie verzamelen over e-mailadressen en zelfs wachtwoorden en creditcardnummers.

Spyware is vergelijkbaar met een Trojaans paard omdat gebruikers ook in dat geval het product onbewust installeren wanneer ze een ander programma installeren. Een veel voorkomende manier waarbij men het slachtoffer wordt van spyware is bepaalde P2P-programma's voor bestandsuitwisseling te downloaden.

Naast het feit dat deze methode onethisch is en een inbreuk op de privacy van de gebruiker betekent, steelt spyware van de gebruiker door de geheugenbronnen van de computer te gebruiken en bandbreedte te verbruiken wanneer de informatie naar de thuisbasis van de spyware wordt verzonden via de internetverbinding van de gebruiker. Aangezien spyware geheugen- en systeemgeheugen gebruikt, kunnen de toepassingen die op de achtergrond worden uitgevoerd leiden tot systeemfouten of een algemene systeeminstabiliteit.

Startup items

Elk bestand in deze map wordt geopend wanneer de computer wordt gestart. Een opstartitem kan bijvoorbeeld een opstartscherm zijn, een geluidsbestand dat moet worden afgespeeld wanneer de computer voor de eerste maal opstart, een herinneringsagenda of apps. In normale omstandigheden wordt een alias van een bestand in deze map geplaatst, en niet het bestand zelf.

Abonnement

Koopovereenkomst die u het recht heeft om een specifiek(e) product of dienst op een specifiek aantal toestellen en voor een bepaalde tijd te gebruiken. Een vervallen abonnement kan automatisch worden verlengd met gebruik van de informatie van de gebruiker tijdens de eerste aankoop.

Systeemvak

Het systeemvak, dat met Windows 95 werd ingevoerd, bevindt zich in de taakbalk van Windows (doorgaans onderaan naast de klok) en bevat miniatuurpictogrammen die systeemfuncties zoals fax, printer, modem, volume en meer, gemakkelijk toegankelijk maken. Dubbelklik of klik met de rechtermuisknop op een pictogram om de details en de besturingselementen te bekijken en te openen.

TCP/IP

Transmission Control Protocol/Internet Protocol - Een reeks netwerkprotocollen, wijdverspreid gebruikt op het internet, die communicatie bieden tussen onderling verbonden computernetwerken met verschillende hardware-architecturen en diverse besturingssystemen. TCP/IP bevat standaarden voor de manier waarop computers communiceren en regels voor het aansluiten van netwerken en het routeren van het verkeer.

Dreiging

Een programma of een deel van een code die op uw computer wordt geladen zonder uw medeweten en tegen uw wil wordt uitgevoerd. De meeste bedreigingen kunnen zichzelf ook dupliceren. Alle computerbedreigingen zijn door de mens gemaakt. Een eenvoudige bedreiging die zichzelf steeds opnieuw kan dupliceren is relatief eenvoudig te maken. Zelfs een dergelijke eenvoudige bedreiging is gevaarlijk aangezien het snel al het beschikbare geheugen zal opgebruiken en het systeem zal blokkeren. Een nog gevaarlijker type is een bedreiging die in staat is zichzelf te verzenden via netwerken en beveiligingssystemen te omzeilen.

informatie-updates van dreigingen

Het binaire patroon van een bedreiging, gebruikt door de beveiligingsoplossing om de bedreiging te detecteren en te verwijderen.

Trojaans paard

Een destructief programma dat zich voordoet als een goedaardige toepassing. In tegenstelling tot kwaadaardige softwareprogramma's en wormen, vermenigvuldigen Trojaanse paarden zich niet, maar ze kunnen even vernietigend zijn. Een van de meest verraderlijke bedreigingstypes van de Trojaanse paarden is een programma dat beweert dat het uw computer kan bevrijden van bedreigingen, maar dat in werkelijkheid bedreigingen op uw computer installeert.

De naam komt uit een verhaal uit de Ilias van Homerus. De Grieken schonken hun vijanden, de Trojanen, een reusachtig houten paard, zogenaamd als vredesgebaar. Maar nadat de Trojanen het paard binnen de stadsmuren hadden gesleept, kwamen de Griekse soldaten uit de holle romp van het paard tevoorschijn en openden ze de poorten van de stad, zodat hun landgenoten Troje konden binnendringen en veroveren.

Update

Een nieuwe versie van een software- of hardwareproduct, dat werd ontwikkeld om een oudere versie van hetzelfde product te vervangen. Daarnaast zullen de installatieroutines voor updates vaak controleren of er reeds een oudere versie van het product op uw computer is geïnstalleerd. Is dat niet het geval, dan kunt u de update niet installeren.

Bitdefender heeft zijn eigen updatefunctie waarmee u handmatig kunt controleren op updates of die het product automatisch kan updaten.

Virtueel privénetwerk (VPN)

Dit is een technologie die een tijdelijke en versleutelde rechtstreekse verbinding met een zeker netwerk over een minder beveiligd netwerk mogelijk maakt. Op die manier is het verzenden en ontvangen van data veilig en versleuteld, zodat ze moeilijk te vangen is door spionnen. Een bewijs van veiligheid is de authentificatie, die enkel mogelijk is via een gebruikersnaam en wachtwoord.

Worm

Een programma dat zich verspreidt via een netwerk en zichzelf ondertussen reproduceert. Dit type kan zich niet vasthechten aan andere programma's.