GEBRUIKSAANWIJZING

Bitdefender CONSUMER SOLUTIONS

Parental Control

Bitdefender Ouderlijk Toezicht

Handleiding

Publication date 04/29/2024

Kennisgevingen

Bitdefender

Inhoudsopgave

OVER DEZE GIDS

Voor wie is deze handleiding bedoeld?

Deze handleiding is bedoeld voor alle Bitdefender-gebruikers die Bitdefender Ouderlijk toezicht hebben gekozen als hun standaardoplossing voor de veiligheid, monitoring en continue bescherming van de apparaten en online aanwezigheid van hun kinderen.

U zult ontdekken hoe u Bitdefender Ouderlijk toezicht kan installeren, configureren en er het beste van kan maken, voor verbeterde functies en een betere controle over de online activiteiten van uw kind.

We wensen u veel leesplezier met deze handleiding.

Hoe kunt u deze handleiding gebruiken?

De handleiding is ingedeeld aan de hand van enkele hoofdonderwerpen:

Aan de slag (pagina 4)

Ga aan de slag met het instellen van uw Bitdefender Ouderlijk toezicht.

Functies en functionaliteiten (pagina 10)

Leer hoe u Bitdefender Ouderlijk toezicht en al zijn functies kan gebruiken.

Hulp vragen (pagina 22)

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. AAN DE SLAG

We beginnen met een diepgaande, stapsgewijze handleiding voor het instellen van een Bitdefender Ouderlijk toezicht-abonnement op uw Bitdefender Central-account. Dit is de eerste stap in het eenvoudige proces dat nodig is om ervoor te zorgen dat u de online activiteiten van uw kinderen doeltreffend kan beheren en volgen.

1.1. Ouderlijk toezicht instellen

Na het activeren van uw abonnement, om te beginnen met het instellen van Bitdefender Ouderlijk toezicht op uw account:

1. Ga naar uw Bitdefender Central-account en ga naar het tabblad **Ouderlijk toezicht** aan de linkerkant van het scherm.
2. Klik op **Aan de slag**.
3. Applicatie-pincode instellen

   > **Belangrijk**
   > Deze pincode helpt voorkomen dat uw kinderen zelf functies voor ouderlijk toezicht uitschakelen door uit te loggen bij hun kinder-app.
   >
   > Zorg ervoor dat u deze pin onthoudt.

4. Klik op **Volgende**.
5. Ga verder met het aanmaken van een kindprofiel. Typ de naam van het kind en selecteer een profielfoto. Klik dan op **Volgende**.
6. Selecteer de leeftijd die overeenkomt met die van uw kind. Klik daarna op **volgende**.
7. Geef aan of de app Ouderlijk toezicht moet worden geïnstalleerd op het huidige apparaat dat u gebruikt of op een ander apparaat.

Belangrijk

Als u **Andere apparaten** selecteert, krijgt u drie installatie-opties te zien. Selecteer de gewenste methode:

- Door de QR-code te scannen.
- Door de verstrekte link te kopiëren en te openen in de browser op het apparaat van het kind.
- Door de installatielink via e-mail te verzenden.

8. Wacht tot de download is voltooid en voer vervolgens het installatieprogramma uit op het betreffende apparaat.

Vanaf hier begint het installatieproces. De stappen die vanaf hier moeten worden genomen, variëren op basis van het type apparaat en het besturingssysteem waarop de installatie wordt uitgevoerd.

1.2. Bitdefender Ouderlijk toezicht installeren op de apparaten van uw kind

1.2.1. Op Windows-apparaten:

Nadat u het nieuw gedownloade installatieprogramma hebt uitgevoerd:

1. Klik op **Ja** als u in een dialoogvenster Gebruikersaccountbeheer wordt gevraagd om het installatiebestand toe te staan wijzigingen aan te brengen op het apparaat.
2. Meld u aan met de inloggegevens van uw Bitdefender Central-account als daarom wordt gevraagd.

1.2.2. Op macOS-apparaten:

Zodra het downloaden van het installatieprogramma is voltooid, dubbelklikt u op het Bitdefender-bestand om het installatieproces te starten:

1. U wordt door de stappen geleid die nodig zijn om Bitdefender Ouderlijk toezicht voor macOS te installeren. Klik op **Toestaan** als daarom wordt gevraagd.
2. Klik op de twee opeenvolgende knoppen **Doorgaan**.

3. Om door te gaan met de installatie, moet u akkoord gaan met de voorwaarden van de abonnementsovereenkomst van de software.
4. Klik op **Doorgaan**. Klik daarna op **Installeren**.
5. Voer desgevraagd een beheerdersnaam en wachtwoord in en druk vervolgens op de knop **Software installeren**.

Wacht tot u een pop-upmelding ontvangt dat *een systeemextensie werd geblokkeerd*. Dit is een natuurlijk verschijnsel tijdens deze procedure. Om door te gaan, moet u de systeemextensie voor Ouderlijk toezicht toestaan volgens de onderstaande instructies:

1. Klik op de knop **Systeeminstellingen openen**.

> **Belangrijk**
> Op een eerdere macOS-versie wordt deze knop aangeduid als **Open beveiligingsvoorkeuren**.

2. Klik op de knop **Toestaan** in de vensters die op het scherm verschijnen, en voer vervolgens de naam en het wachtwoord van een beheerder in om de instellingen te ontgrendelen.

> **Belangrijk**
> In macOS 11 (Big Sur) en macOS 12 (Monterey) moet u, voordat u op de knop **Toestaan** kan klikken, eerst op het hangslotsymbool in de linkerbenedenhoek van het venster **Beveiliging en privacy** klikken en vervolgens de naam en het wachtwoord van een beheerder invoeren om wijzigingen aan te brengen.

3. Het pop-upvenster **Netwerkinhoud filteren** verschijnt. Klik op de knop **Toestaan** in dit venster.
4. Klik vervolgens op de knop **Systeeminstellingen openen**.
5. Klik nog een keer op de knop **Toestaan**.

1.2.3. Op Android-apparaten:

U vindt de Google Play Store-pagina van Bitdefender voor de applicatie Ouderlijk toezicht:

1. Tik op de knop **Installeren**. De app wordt gedownload en geïnstalleerd.

2. Zodra de installatie is voltooid, ziet u een knop **Openen**. Tik erop om de Bitdefender Ouderlijk toezicht-applicatie te starten.

Volg na het openen van de applicatie de stappen op het scherm om Ouderlijk toezicht in te stellen op het Android-apparaat van uw kind:

1. Tik op **Doorgaan**.
2. Meld u aan bij de app met de inloggegevens van uw Bitdefender Central-account.
3. Selecteer het kindprofiel dat u aan het Android-apparaat wilt toewijzen.
4. U moet de nodige machtigingen verlenen om de app goed te laten functioneren. Tik hiervoor op **Volgende** en vervolgens:
   a. Sta VPN-toegang toe en kies vervolgens **Altijd toestaan** om online inhoud op het apparaat van uw kind te filteren.
   b. Om het Android-apparaat van uw kind te lokaliseren, tikt u op **Volgende**, vervolgens op **Toestaan**, en kiest u de optie **Altijd toestaan**.
   c. Zowel VPN- als locatiemachtigingen krijgen een groen vinkje. Tik op **Installatie voltooien** en tik vervolgens op **Volgende**.
   d. Op dit punt zijn er nog 3 machtigingen om internettoegang en apps op het apparaat van het kind te blokkeren. Tik op **Machtiging instellen** in het deelvenster **Apparaatbeheerdersrechten**.
   e. Tik op de knop **Voltooien** zodra u klaar bent met het instellen van de Bitdefender-app voor Ouderlijk toezicht.

1.2.4. Op iOS-apparaten:

U vindt de App Store-pagina van Bitdefender voor de applicatie Ouderlijk toezicht:

1. Tik op het wolkpictogram met een pijl die naar beneden wijst. De applicatie wordt gedownload en geïnstalleerd.
2. Zodra de installatie is voltooid, ziet u een knop **Openen**. Tik erop om de Bitdefender Ouderlijk toezicht-app te starten.

3. Als er beheerprofielen van mobiele apparaten worden gevonden op het iOS-apparaat van het kind, wordt u gevraagd deze te verwijderen. Tik op **Volgende** en kies **Profielen verwijderen**.
4. Ga in de **Instellingen**-app van iOS naar **Algemeen**, scrol omlaag en tik op de sectie **VPN- en Apparaatbeheer**.
5. Tik op elk item in de sectie **BEHEER VAN MOBIELE APPARATEN** en kies **Beheer verwijderen** voor elk ervan.
   Herhaal dit proces totdat er geen items in BEHEER VAN MOBIELE APPARATEN meer over zijn.

Open de app die op het apparaat van het kind is geïnstalleerd opnieuw en volg de stappen op het scherm om Bitdefender Ouderlijk toezicht in te stellen:

1. Tik op **Doorgaan**.
2. Meld u aan bij de app met de inloggegevens van uw Bitdefender Central-account.
3. Selecteer het kindprofiel dat u aan het iOS-apparaat wilt toewijzen.
4. U moet dan de nodige machtigingen verlenen om de applicatie goed te laten functioneren. Tik op **Volgende**.
5. Sta VPN-toegang toe om online inhoud op het apparaat van uw kind te filteren. Tik twee keer achter elkaar op **Toestaan** om de VPN-configuraties toe te voegen.
6. Tik op **Volgende**, en kies **Toestaan** om te helpen bij het lokaliseren van het iOS-apparaat van uw kind.
7. Doorloop vervolgens het proces van het instellen van Delen met gezin van Apple om internettoegang en apps op het apparaat van het kind te blokkeren.

   > **Belangrijk**
   > U kunt tikken op **Leer hoe** voor een stapsgewijze handleiding over hoe u dat moet doen.

8. Nadat u Delen met gezin van Apple hebt geconfigureerd op uw eigen apparaat en op het apparaat van uw kind, selecteert u Ik **heb Delen met gezin van Apple geconfigureerd** om door te gaan.

9. Sta vervolgens toegang tot Schermtijd toe om online inhoud op het iOS-apparaat van uw kind te filteren.
10 Tik op **Installatie voltooien**.

.

Nadat u deze stappen op het (de) apparaat(-aten) van uw kind hebt voltooid, is het installatieproces afgerond. Als ouder kan u nu de online activiteiten van uw kind volgen en gebruiksstatistieken bekijken in uw Bitdefender Central-account, op het dashboard voor Ouderlijk toezicht, dat we in de volgende hoofdstukken zullen beschrijven.

2. FUNCTIES EN FUNCTIONALITEITEN

2.1. Profielen

Een kindprofiel is een aangepaste set regels waarmee de Ouderlijk toezicht-app van Bitdefenderde online activiteiten van een kind kan beheren en monitoren. Het bevat instellingen die zijn afgestemd op de leeftijd van het kind, zoals inhoudsfilters en tijdsbeperkingen. Met behulp van het Bitdefender Central-account kunnen ouders deze profielen aanmaken, bewerken en wissen, en er apparaten aan toewijzen en uit verwijderen, zodat hun kinderen verzekerd zijn van een veilige en gepaste online ervaring.

Een kindprofiel aanmaken:

1. Ga naar Bitdefender Central en meld u aan bij uw account.
2. Klik in het menu aan de linkerkant op het tabblad **Ouderlijk toezicht**.
3. Klik op **Nieuw profiel** om een nieuw kindprofiel aan te maken.
4. Voer de naam, profielfoto en geboortedatum van het kind in.

   > **Belangrijk**
   > Op basis van de leeftijd van het kind blokkeert Bitdefender automatisch bepaalde categorieën, zoals chats, sociale netwerken, expliciete inhoud en meer. U kan geblokkeerde categorieën later aanpassen.

5. Klik op de knop **Opslaan**.

Het nieuwe profiel is nu aangemaakt en verschijnt op de pagina.

Een kindprofiel bewerken:

1. Klik op de knop **Details weergeven** in het profiel van het kind.
2. Als u het profiel van uw kind wilt wijzigen, gaat u naar **Profiel bewerken**.
3. Gebruik het overeenkomstige veld om de naam, geboortedatum en/of profielfoto van het kind te wijzigen.
4. Klik op **Wijzigingen opslaan** na het aanpassen van de nodige gegevens.

Een kindprofiel verwijderen:

1. Klik op de knop **Details weergeven** in het profiel van het kind.
2. Ga naar **Profiel bewerken**.
3. Klik op de knop **Profiel verwijderen** en bevestig de verwijdering.

Apparaten toewijzen aan een kindprofiel:

Als uw kind meerdere apparaten heeft (Windows, macOS, Android of iOS), kan u deze toewijzen aan hetzelfde kindprofiel.

1. Klik op de knop **Details weergeven** in het profiel van het kind.
2. Klik op het aantal apparaten dat onder hun naam wordt vermeld.
3. Klik op de knop **Apparaten toewijzen**.
4. Selecteer de apparaatnaam en klik vervolgens op de knop **Toewijzen**.

> **Belangrijk**
> Als het apparaat niet in de lijst staat, klikt u op **Een nieuw apparaat installeren** en volgt u de instructies op het scherm om Ouderlijk toezicht van Bitdefender op het nieuwe apparaat te installeren en in te stellen.

Apparaten verwijderen uit een kindprofiel:

Wanneer u een apparaat uit het profiel van een kind verwijdert, betekent dit dat het apparaat niet langer onder het beheer van Bitdefender Ouderlijk toezicht valt. De regels en instellingen die in het profiel van het kind zijn opgegeven, zijn niet meer van toepassing op dat apparaat. Hoewel de app Ouderlijk toezicht op het apparaat geïnstalleerd blijft, werkt deze niet meer.

1. Klik op de knop **Details weergeven** in het profiel van het kind.
2. Klik op het aantal apparaten dat onder hun naam wordt vermeld.
3. Lokaliseer het apparaat van het kind en klik op de optie **Apparaat niet langer toewijzen**.
4. Druk op de knop **Ja, apparaat niet langer toewijzen** om de actie te bevestigen.

2.2. Statistieken

Ouderlijk toezicht geeft inzicht in hoe kinderen internet en hun apparaten gebruiken. In deze handleiding gaan we dieper in op de verschillende

statistieken die beschikbaar zijn voor ouders in Bitdefender Central, zodat ze weloverwogen beslissingen kunnen nemen en een veilige en evenwichtige online ervaring voor hun kinderen kunnen garanderen.

Om de statistieken te bekijken:

1. Ga naar Bitdefender Central en meld u aan bij uw account.
2. Nadat u bent ingelogd, klikt u op het tabblad **Ouderlijk toezicht** in het menu aan de linkerkant.
3. Klik op het profiel van het kind waarvan u de statistieken wilt bekijken.

Nadat u het profiel van uw kind hebt geselecteerd, wordt u doorverwezen naar een dashboard met verschillende statistiekvensters. Ze verwijzen allemaal naar de andere functies die verderop in deze documentatie worden beschreven.

2.3. Pincode van het ouderlijk toezicht

De pincode voor ouders is een beveiligingsfunctie binnen het dashboard voor Ouderlijk toezicht van het Bitdefender Central-platform. Het dient als een middel voor ouders om controle te houden over de toegang van hun kind tot de Bitdefender Ouderlijk toezicht-app die op hun apparaten is geïnstalleerd. Hieronder vindt u een gedetailleerde handleiding voor het instellen, vinden en beheren van uw pincode voor ouders.

Met de pincode voor ouders voorkomt u ongeoorloofde afmeldingen bij de Bitdefender Ouderlijk toezicht-app op het apparaat van uw kind. Wanneer uw kind probeert uit te loggen, wordt het gevraagd deze pincode in te voeren. Het zorgt ervoor dat alleen u, als ouder met toegang tot het Bitdefender Central-account, de instellingen van de app kan beheren.

> **Belangrijk**
> Wanneer u de app Ouderlijk toezicht voor de eerste keer instelt, wordt u gevraagd om een 4-8-cijferige pincode voor ouders in te stellen.

2.3.1. Pincode vergeten?

Als u uw pincode voor ouders vergeet, kan u deze eenvoudig ophalen uit uw Bitdefender Central-account:

1. Ga naar Bitdefender Central en meld u aan bij uw account.

2. Nadat u bent ingelogd, klikt u op het tabblad **Ouderlijk toezicht** in het menu aan de linkerkant.
3. Klik in de rechterbovenhoek van de pagina op **Pincode**.
4. Klik op het oogvormige pictogram om uw pincode voor ouders te vinden.

2.3.2. Uw pincode wijzigen

Als u vermoedt dat uw pincode is gecompromitteerd of deze om veiligheidsredenen wilt bijwerken:

1. Klik in de sectie Ouderlijk toezicht van uw Bitdefender Central-account op de optie **Pincode**.
2. Kies de optie **Pincode wijzigen** en volg de aanwijzingen op uw scherm om een nieuwe pincode in te stellen.

2.4. Inhoudsfiltering

Met Inhoudsfiltering kunnen ouders de toegang van hun kind tot online inhoud beperken, zodat ze hele categorieën websites kunnen blokkeren of uitzonderingen kunnen maken op basis van specifieke URL's of onderwerpen.

> **Belangrijk**
> De functie voor het filteren van inhoud van Bitdefender Ouderlijk toezicht weerhoudt uw kind er niet van om applicaties van websites offline te gebruiken, aangezien het alleen het online internetverkeer beheert van de apparaten die ze gebruiken.

Om toegang te krijgen tot Inhoudsfiltering:

1. Meld u aan op uw Bitdefender Central-account.
2. Klik in het menu aan de linkerkant op het tabblad **Ouderlijk toezicht**.
3. Ga naar het profiel van uw kind en klik rechtsboven op het menu **Meer**. Selecteer vervolgens **Inhoudsfiltering**.

2.4.1. Veilig zoeken en YouTube-beperkingen

In de sectie **Privacy en veiligheid** aan de rechterkant van het scherm kan u de schakelaars Safe Search (veilig zoeken) en YouTube Restricted (beperkte YouTube) inschakelen.

- **Safe Search:** Bij het gebruik van zoekmachines voorkomt Safe Search dat inhoud die door Google als onveilig wordt beschouwd, wordt weergegeven in zoekresultaten.
- **YouTube restricted:** Biedt het kind video's op YouTube die geschikt zijn voor de leeftijd.

> **Belangrijk**
> **Safe Search** en **YouTube restricted** leiden alle DNS-verzoeken van **google.com** om naar **safe.google.com**. Het eigenlijke filteren van inhoud wordt gedaan door Google. Bitdefender Ouderlijk toezicht filtert geen inhoud binnen Safe Search of Google. Ook is het mogelijk dat YouTube tags op video's niet effectief controleert, waardoor kinderen mogelijk worden blootgesteld aan ongepaste inhoud.

2.4.2. Websitecategorieën blokkeren en toestaan

> **Belangrijk**
> In de sectie **Categorieën** zijn de typen websites die uw kind online kan zien, standaard toegestaan of geblokkeerd, afhankelijk van de leeftijd die is ingesteld toen het profiel van het kind werd gemaakt.

U kan op elk gewenst moment verschillende soorten websites blokkeren of toestaan:

1. Selecteer een categorie.
2. Als u de toegang tot deze categorie wilt blokkeren, kiest u **Geblokkeerd** in het vervolgkeuzemenu. Als u toegang wilt toestaan, kiest u **Toegestaan**.

> **Belangrijk**
> Als u de categorie **Bestandsdeling** voor het profiel van uw kind blokkeert, werkt de macOS-update niet. We raden aan om Bestandsdeling tijdelijk toe te staan bij het updaten van macOS.

2.4.3. Uitzonderingen

Op het tabblad **Uitzonderingen** kunnen uitsluitingen voor websites en applicaties worden ingesteld:

- **Website-uitzonderingen:**
  1. Klik op de knop **Uitzondering toevoegen**.

2. Selecteer **Alleen website** en klik vervolgens op de knop **Volgende**.
3. Typ het websiteadres en selecteer of u het wilt toestaan of blokkeren in het vervolgkeuzemenu.
4. Klik vervolgens op de knop **Toevoegen**.

- **Uitzonderingen voor app en webplatform:**
  1. Klik op de knop **Uitzondering toevoegen**.
  2. Selecteer **App en webplatform** en klik vervolgens op de knop **Volgende**.
  3. Kies het platform waarvoor u een uitzondering wilt maken uit de verstrekte lijst. U kan ook de zoekbalk gebruiken om te vinden wat u zoekt.
  4. Klik vervolgens op de knop **Toevoegen**.

- **Uitzonderingen verwijderen:**
  Alle uitzonderingen die u instelt, worden weergegeven in Inhoudsfiltering in de daarvoor bestemde lijst onderaan.
  Om een uitzondering te verwijderen, klikt u gewoon op het prullenbakpictogram rechts van het item.

2.5. Dagelijkse internettijd

In uw Bitdefender Central-account onder de sectie Ouderlijk toezicht wordt voor elk aangemaakt kindprofiel een kaart met dagelijkse internettijd weergegeven. Deze kaart toont de totale tijd die het kind online heeft doorgebracht op alle toegewezen apparaten. De online tijd van een kind beperken:

1. Ga naar het kindprofiel en klik op de knop **Tijdsbeperking instellen** in het deelvenster **Dagelijkse internettijd**. U kan ook op het menu **Meer** in de rechterbovenhoek klikken en **Dagelijkse internettijd** selecteren.
2. Klik op de knop **Tijdslimiet inschakelen** om deze functie te activeren.

Belangrijk

Standaard krijgt het kind 1 uur en 30 minuten internettoegang per dag. Als de ouder deze tijdsbeperking niet verlengt, wordt de internettoegang van het kind stopgezet na het bereiken van de limiet van 1 uur en 30 minuten.

Dagelijkse tijdsbeperking verwijderen:

- Om de functie Dagelijkse internettijd uit te schakelen, gaat u naar het dashboard van het profiel van uw kind, klikt u op de knop **Tijd bewerken** in het deelvenster **Dagelijkse internettijd** en drukt u vervolgens op de knop **Pauze** in het deelvenster **Tijdslimiet**.
- Als u de tijdsbeperking voor een bepaalde dag wilt verwijderen, klikt u op de knop ⊗ die overeenkomt met die dag van de week in het deelvenster **Planning**.

Tijdsbeperking wijzigen:

- Als u een andere tijdsbeperking voor een specifieke dag van de week wilt instellen, klikt u op de naam van de dag in het deelvenster **Planning**, selecteert u de gewenste limiet in het vervolgkeuzemenu en klikt u vervolgens op de knop **Wijzigingen opslaan**. U kan meer dan één dag tegelijk selecteren.

2.5.1. Beloningssysteem

Met de functie **Beloning** kan u uw kind belonen of de schermtijd verlengen om gezonde online gewoonten te stimuleren. U kan het beloningssysteem op twee verschillende manieren gebruiken:

- **Handmatige beloning:**
  1. Navigeer door de sectie Ouderlijk toezicht in uw Bitdefender Central-account.
  2. Ga naar het kindprofiel en klik op de knop **Beloning** in het deelvenster **Dagelijkse internettijd**.
  3. Selecteer de hoeveelheid extra tijd die u wilt toevoegen en bevestig door op **Beloning** te klikken.
- **Verzoek van het kind:**
  Wanneer uw kind de dagelijkse limiet bereikt, kan het extra tijd aanvragen via de app Ouderlijk toezicht die op hun mobiele apparaat

is geïnstalleerd. Als ouder ontvangt u een melding in uw Bitdefender Central-account.

1. Wanneer u bent ingelogd op uw Bitdefender Central-account, zoekt u naar een rode stip op de meldingsbel in de rechterbovenhoek van het scherm, die aangeeft dat uw kind een verzoek in behandeling heeft.
2. Bekijk de aanvraag en beslis hoeveel extra tijd u wilt toekennen.

> **Belangrijk**
> Kinderen hebben alleen op Android- en iOS-apparaten de mogelijkheid om verlengingen van hun dagelijkse internettijd aan te vragen.

2.6. Het internet uitschakelen op het apparaat van uw kind

Als ouder kan het beheren van het internetgebruik van uw kind belangrijk zijn voor hun welzijn en productiviteit. Om de internettoegang op het apparaat van uw kind tijdelijk uit te schakelen met Bitdefender Ouderlijk toezicht:

1. Ga naar Bitdefender Central en meld u aan bij uw account.
2. Nadat u bent ingelogd, klikt u op het tabblad **Ouderlijk toezicht** in het menu aan de linkerkant.
3. Selecteer **Details weergeven** in het profiel van het kind van wie u het internet wilt uitschakelen.
4. Klik op de knop **Internet stoppen** in de rechterbovenhoek van het dashboard van het kind

> **Belangrijk**
> Het internet wordt afgesloten op alle apparaten van uw kind. Deze actie overschrijft alle bestaande instellingen voor Ouderlijk toezicht, zoals routines, dagelijkse tijdsbeperking of toegestane categorieën.

5. Terwijl de toegang tot internet wordt verbroken, wordt de knop **Internet stoppen** gewijzigd in **Internet hervatten**. Om de

internettoegang te herstellen, klikt u gewoon op de knop **Internet hervatten**.

2.7. Routines

Binnen Bitdefender Ouderlijk toezicht kan u tot 3 verschillende routines instellen om te plannen wanneer de internettoegang van uw kind wordt uitgeschakeld. Ze bieden een gestructureerde aanpak voor het beheren van de online activiteiten van een kind, het bevorderen van gezonde gewoonten en gezinsbetrokkenheid en het waarborgen van hun veiligheid. Deze routines zijn onafhankelijk van elkaar, wat betekent dat u ervoor kan kiezen om slechts één, twee of alle drie te activeren, afhankelijk van uw voorkeuren:

- **Focustijd**
  Maak een planning met tijd voor huiswerk, studie en andere activiteiten.
- **Bedtijd**
  Gebruik de bedtijdroutine om een rustperiode voor uw kind vast te leggen.
- **Familietijd**
  Gebruik de Familietijd-routine om tijd vrij te maken voor uw kind om bijvoorbeeld aanwezig te zijn tijdens gezinsmaaltijden.

> **Belangrijk**
> **Routines versus Dagelijkse internettijd:**
>
> Tijdens routines telt de tijd die online wordt doorgebracht niet mee voor de dagelijkse internettijdsbeperking. Zodra de routine is afgelopen, hervat de functie Dagelijkse internettijd het tellen van het internetgebruik van het kind.
>
> Om verwarring bij ouders te voorkomen, is de kaart Dagelijkse internettijd tijdens een routine pas zichtbaar op het dashboard van het profiel van het kind als de routine is voltooid. In plaats daarvan wordt gedurende deze tijd de naam van de actieve routine weergegeven.

2.7.1. Routines instellen

Instellen van de routines van het Ouderlijk toezicht:

1. Ga naar Bitdefender Central en meld u aan bij uw account.

2. Klik in het menu aan de linkerkant op het tabblad **Ouderlijk toezicht**.
3. Ga naar het kindprofiel en selecteer een gewenste routine in het menu **Meer**.
4. Klik op de knop **Inschakelen** om de geselecteerde routine te activeren.
5. Hierdoor worden de deelvensters **Planning** en **Internettoegang** weergegeven.

   - **Planning:**
     Een routine instellen voor één of meerdere dagen van de week:

     a. Selecteer de gewenste dagen.

     b. Selecteer de begin- en eindtijd voor de routine in het vervolgkeuzemenu.

     c. Klik ten slotte op de knop **Wijzigingen opslaan** om uw selecties te bevestigen.

     Om de routine voor een bepaalde dag te verwijderen, klikt u op de knop ⊗ die overeenkomt met die dag van de week.

   - **Internettoegang:**
     Het deelvenster Internettoegang binnen een routine biedt twee hoofdfuncties om de online activiteiten van een kind gedurende specifieke tijdsbestekken te beheren:

     - **Volledige internetafsluiting:** Ouders hebben de mogelijkheid om de internettoegang voor hun kind volledig uit te schakelen tijdens de geplande routinetijd. Door de schakelaar **Internettoegang** uit te schakelen, hebben de apparaten van het kind geen toegang tot internet binnen het aangegeven tijdsbestek.

     - **Selectieve categorie of website:** Ouders kunnen er ook voor kiezen om internettoegang toe te staan tijdens routine-uren, maar bepaalde websites of inhoudscategorieën te beperken. Wanneer u de schakelaar **Internettoegang** inschakelt, worden twee extra tabbladen, namelijk de tabbladen **Categorieën** en **Uitzonderingen**, zichtbaar, waardoor u toegang krijgt tot verdere instellingen voor Inhoudsfiltering</link>. (pagina 13)

2.8. De locatie van uw kind traceren

Met de prevalentie van smartphones en andere mobiele apparaten is het traceren van de locatie van kinderen voor veel gezinnen een essentieel hulpmiddel geworden. Of het nu gaat om weten waar ze zijn na school of tijdens uitstapjes met vrienden, de mogelijkheid om hun locatie te traceren, zorgt voor gemoedsrust bij de ouders. Hier is een stap-voor-stap handleiding over hoe u de locatie van uw kind kunt traceren met behulp van de locatiefunctie van Bitdefender Ouderlijk toezicht.

1. Ga naar Bitdefender Central en meld u aan bij uw account.
2. Nadat u bent ingelogd, klikt u op **Ouderlijk toezicht** in het menu aan de linkerkant.
3. Als u meerdere kinderen hebt, selecteert u **Details weergeven** in het profiel van het kind waarvan u de locatie wilt traceren.
4. Selecteer in het deelvenster Locatie het Android- of iOS-apparaat dat u wilt volgen en klik vervolgens op de knop **Lokaliseren**.

   Belangrijk
   De locatiefunctie in Bitdefender Ouderlijk toezicht is niet beschikbaar voor Windows- en macOS-apparaten.

5. Na een korte wachttijd geeft een rode pin de huidige locatie van uw kind op de kaart aan.

   Belangrijk
   Locatie-updates vinden elke 20 minuten plaats. Als u de locatie van uw kind probeert te volgen in minder dan 20 minuten sinds de vorige locatiebepaling, geeft de weergegeven locatie mogelijk niet in realtime weer waar uw kind zich bevindt.

3. OUDERLIJK TOEZICHT DE-INSTALLEREN

Bitdefender Ouderlijk toezicht de-installeren op Windows-apparaten:

1. Verwijder het apparaat uit het profiel van uw kind in Bitdefender Central.
2. Open het Configuratiescherm op het apparaat in kwestie en zoek Bitdefender Ouderlijk toezicht in de lijst **Programma's en functies**.
3. Bitdefender Ouderlijk toezicht de-installeren.

Bitdefender Ouderlijk toezicht de-installeren op macOS-apparaten:

1. Verwijder het apparaat uit het profiel van uw kind in Bitdefender Central.
2. Open **Finder** op het macOS-apparaat.
3. Open uw applicaties en zoek de Bitdefender-map.
4. Open deze en voer **Bitdefender Uninstaller** uit.
5. Kies Bitdefender Ouderlijk toezicht uit de lijst met te de-installeren producten.
6. Geef de inloggegevens van beheerder op, en wacht tot de de-installatie is voltooid.

Bitdefender Ouderlijk toezicht de-installeren op Android- en iOS-apparaten:

1. Verwijder het apparaat uit het profiel van uw kind in Bitdefender Central.
2. De-installeer Ouderlijk toezicht van het mobiele apparaat zoals elke andere applicatie of via respectievelijk Google Play Store of Appstore.

4. HULP VRAGEN

4.1. 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.

4.2. 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.

4.2.1. 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/.

4.2.2. 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/

4.2.3. 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/.

4.3. 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/

4.3.1. 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.