MANUALE D'USO

Bitdefender CONSUMER SOLUTIONS

Parental Control

Bitdefender Parental Control

Manuale d'uso

Publication date 04/29/2024

Avvertenze legali

Bitdefender

Indice

Informazioni su questa guida 1
Finalità e destinatari 1
Come usare questo manuale 1
Convenzioni usate in questo manuale 1
Convenzioni tipografiche 1
Avvertenze 2
Richiesta di commenti 2
1. Come iniziare 4
1.1. Configurare Parental Control 4
1.2. Installare Bitdefender Parental Control sui dispositivi del bambino 5
1.2.1. Sui dispositivi Windows: 5
1.2.2. Sui dispositivi macOS: 5
1.2.3. Su dispositivi Android: 6
1.2.4. Sui dispositivi iOS: 7
2. Funzionalità e caratteristiche 9
2.1. Profili 9
2.2. Statistiche 10
2.3. Codice PIN parentale 11
2.3.1. Hai dimenticato il codice PIN? 11
2.3.2. Modificare il tuo codice PIN 12
2.4. Filtro contenuti 12
2.4.1. Ricerca sicura e restrizioni di YouTube 12
2.4.2. Blocco e autorizzazione delle categorie di siti web 13
2.4.3. Eccezioni 13
2.5. Tempo quotidiano su Internet 14
2.5.1. Sistema di ricompense 15
2.6. Disattivare Internet sul dispositivo del bambino 16
2.7. Routine 16
2.7.1. Impostare le routine 17
2.8. Tracciamento della posizione del bambino 18
3. Disinstallare Parental Control 20
4. Ottenere aiuto 21
4.1. Richiesta d'aiuto 21
4.2. Risorse online 21
4.2.1. Centro di supporto di Bitdefender 21
4.2.2. La community di esperti di Bitdefender 22
4.2.3. Bitdefender Cyberpedia 22
4.3. Informazioni di contatto 23

4.3.1. Distributori locali 23
Glossario 24

INFORMAZIONI SU QUESTA GUIDA

Finalità e destinatari

Questa guida è destinata a tutti gli utenti Bitdefender che hanno scelto Bitdefender Parental Control come soluzione di riferimento per la sicurezza, il monitoraggio e la protezione continua dei dispositivi e della presenza online dei bambini.

Scoprirai come installare, configurare e sfruttare al meglio Bitdefender Parental Control per usufruire di funzionalità avanzate e un miglior controllo sulle attività online del bambino.

Buona lettura e speriamo che lo troverai utile.

Come usare questo manuale

Questo manuale presenta alcuni argomenti principali:

Come iniziare (pagina 4)

Inizia a configurare Bitdefender Parental Control.

Funzionalità e caratteristiche (pagina 9)

Scopri come utilizzare Bitdefender Parental Control e tutte le sue funzionalità.

Ottenere aiuto (pagina 21)

Dove cercare e ottenere aiuto in caso di difficoltà o problemi.

Convenzioni usate in questo manuale

Convenzioni tipografiche

Nel manuale vengono usati diversi stili di testo per migliorare la leggibilità. L'aspetto e il significato sono illustrati nella tabella sottostante.

Aspetto	Descrizione
sample syntax	Gli esempi di sintassi vengono stampati con monospaced caratteri.
https://www.bitdefender.com	I link URL indirizzano a una qualche ubicazione esterna, su server http o ftp.
documentation@bitdefender.com	Gli indirizzi e-mail vengono inseriti nel testo come informazioni di contatto.
A proposito di questa guida (pagina 1)	Questo è un link interno, verso una qualche ubicazione nel documento.
filename	File e directory vengono stampati utilizzando monospaced font.
opzione	Tutte le opzioni del prodotto vengono stampate utilizzando **grassetto** caratteri.
parola chiave	Le parole chiave o le frasi importanti vengono evidenziate utilizzando **grassetto** caratteri.

Avvertenze

Le avvertenze appaiono sotto forma di note di testo, segnalate graficamente, portando alla tua attenzione ulteriori informazioni relative al paragrafo attuale.

Nota

Le note sono solo piccole osservazioni. Anche se si possono omettere, le note potrebbe fornire informazioni preziose, come una determinata caratteristica o un link verso eventuali temi collegati.

Importante

Richiede la tua attenzione e non è consigliato ignorarla. Solitamente, fornisce informazioni non critiche ma importanti.

Avvertimento

Si tratta di un'informazione critica che dovresti trattare con maggiore cautela. Se segui le istruzioni, non accadrà nulla di male. Dovresti leggerla e comprenderla, perché descrive qualcosa di estremamente rischioso.

Richiesta di commenti

Ti invitiamo ad aiutarci a migliorare il presente manuale. Abbiamo provato e verificato tutte le informazioni con la massima attenzione. Ti preghiamo di scriverci per indicarci eventuali errori che dovessi riscontrare nel manuale o suggerirci come poterlo migliorare, per aiutarci a fornirti la migliore documentazione possibile.

Segnalacelo inviando una mail a documentation@bitdefender.com. Scrivi tutte le tue e-mail relative alla documentazione in inglese in modo che possiamo elaborarle in modo efficiente.

1. COME INIZIARE

Inizieremo con una guida approfondita e passo passo su come configurare l'abbonamento a Bitdefender Parental Control nel tuo account di Bitdefender Central. Si tratta del primo passo del semplice processo necessario per gestire e monitorare in maniera efficace le attività online dei bambini.

1.1. Configurare Parental Control

Dopo aver attivato l'abbonamento, per iniziare a configurare Bitdefender Parental Control sul tuo account:

1. Vai al tuo account di Bitdefender Central e accedi alla scheda **Parental Control** sul lato sinistro dello schermo.
2. Clicca su **Iniziare**.
3. Imposta un PIN dell'applicazione.

   > **Attenzione**
   > Il codice PIN consente di impedire ai bambini di disattivare autonomamente le funzionalità di controllo genitori disconnettendosi dall'applicazione per i bambini.
   >
   > Assicurati di ricordarti tale PIN.

4. Clicca su **Avanti**.
5. Procedi creando un profilo bambino. Inserisci il nome del bambino e seleziona un'immagine del profilo. Poi clicca su **Avanti**.
6. Seleziona l'età che corrisponde a quella del bambino. Una volta fatto, clicca su **Avanti**.
7. Indica se l'app Parental Control deve essere installata sul dispositivo attuale che stai utilizzando o su un altro dispositivo.

Attenzione

Se selezioni **Altri dispositivi**, ti saranno presentate tre opzioni di installazione. Seleziona il metodo che preferisci:

- Scansionando il codice QR.
- Copiando il link fornito e aprendolo nel browser del dispositivo del bambino.
- Inviando il link di installazione via e-mail.

8. Attendi il completamento del download, quindi esegui il programma di installazione sul dispositivo in questione.

Da qui, inizierà il processo di installazione. D'ora in avanti, i passaggi da seguire possono variare in base al tipo di dispositivo e al sistema operativo su cui viene eseguita l'applicazione.

1.2. Installare Bitdefender Parental Control sui dispositivi del bambino

1.2.1. Sui dispositivi Windows:

Una volta eseguito il programma di installazione appena scaricato:

1. Clicca su **Sì** se una finestra di dialogo di controllo dell'account utente ti chiede di consentire al file di installazione di apportare modifiche al dispositivo.
2. Accedi con le credenziali del tuo account di Bitdefender Central, se richiesto.

1.2.2. Sui dispositivi macOS:

Una volta completato il download del programma di installazione, clicca due volte sul file di Bitdefender per avviare il processo di installazione:

1. Ti guideremo nei vari passaggi necessari per installare Bitdefender Parental Control per macOS. Clicca su **Consenti**, se richiesto.
2. Clicca sui due pulsanti **Continua** consecutivi.
3. Per continuare l'installazione, dovrai accettare i termini dell'accordo di abbonamento del software.
4. Clicca su **Continua**. Successivamente, clicca su **Installa**.

5. Quando richiesto, inserisci il nome e la password dell'amministratore, quindi premi il pulsante **Installa software**.

Attendi fino a quando non ricevi una notifica pop-up che indica che *un'estensione di sistema è stata bloccata*. Si tratta di un evento normale durante questa procedura. Per continuare, devi consentire l'estensione di sistema Parental Control secondo le istruzioni riportate di seguito:

1. Clicca sul pulsante **Apri impostazioni di sistema**.

> **Attenzione**
> Nelle versioni precedenti di macOS, questo pulsante viene definito **Apri preferenze di sicurezza**.

2. Clicca sul pulsante **Consenti** nelle finestre visualizzate sullo schermo, quindi inserisci il nome e la password di un amministratore per sbloccare le impostazioni.

> **Attenzione**
> Su macOS 11 (Big Sur) e macOS 12 (Monterey), prima di poter cliccare sul pulsante **Consenti**, dovrai prima cliccare sull'icona del lucchetto nell'angolo in basso a sinistra della finestra **Privacy e Sicurezza**, quindi inserisci il nome e la password dell'amministratore per apportare modifiche.

3. Comparirà la finestra pop-up **Filtra contenuto di rete**. Clicca sul pulsante **Consenti** in questa finestra.
4. Quindi, clicca sul pulsante **Apri impostazioni di sistema**.
5. Clicca sul pulsante **Consenti** ancora una volta.

1.2.3. Su dispositivi Android:

Troverai la pagina di Google Play Store di Bitdefender per l'applicazione Parental Control:

1. Tocca il pulsante **Installa**. La app sarà quindi scaricata e installata.
2. Una volta completata l'installazione, vedrai il pulsante **Apri**. Toccalo per avviare la app Bitdefender Parental Control.

Dopo aver aperto l'applicazione, segui i passaggi sullo schermo per configurare Parental Control sul dispositivo Android del bambino:

1. Tocca **Continua**.
2. Accedi alla app utilizzando le credenziali del tuo account di Bitdefender Central.
3. Seleziona il profilo bambino che vuoi assegnare al dispositivo Android.
4. Dovrai concedere le autorizzazioni necessarie per la app affinché funzioni correttamente. Per farlo, tocca **Avanti**, quindi:
   a. Consenti l'accesso a VPN, poi seleziona **Consenti sempre** per filtrare i contenuti online sul dispositivo del bambino.
   b. Per aiutare a individuare il dispositivo Android del bambino, tocca **Avanti**, poi **Consenti** e seleziona l'opzione **Consenti sempre**.
   c. Sia l'autorizzazione VPN che Posizione visualizzeranno un segno di spunta verde. Tocca **Termina configurazione** e quindi tocca **Avanti**.
   d. A questo punto, ci sono altre 3 autorizzazioni per bloccare l'accesso a Internet e le app sul dispositivo del bambino. Tocca **Imposta autorizzazione** nel pannello **Diritti amministratore dispositivo**.
   e. Tocca il pulsante **Fine** una volta terminata la configurazione della app Bitdefender Parental Control.

1.2.4. Sui dispositivi iOS:

Troverai la pagina di App Store di Bitdefender per l'applicazione Parental Control:

1. Tocca l'icona della nuvola con una freccia rivolta verso il basso. L'applicazione sarà quindi scaricata e installata.
2. Una volta completata l'installazione, vedrai il pulsante **Apri**. Toccalo per avviare la app Bitdefender Parental Control.
3. Se sul dispositivo iOS del bambino vengono trovati eventuali profili di Mobile Device Management, ti sarà chiesto di rimuoverli. Tocca **Avanti** e seleziona **Rimuovi profili**.
4. Nella app **Impostazioni** di iOS, vai in **Generali** e scorri verso il basso, poi tocca la sezione **VPN e Device Management**.
5. Tocca ciascuna voce nella sezione **MOBILE DEVICE MANAGEMENT** e seleziona **Rimuovi management** per ognuna.

Ripeti questo processo finché non ci sono più voci MOBILE DEVICE MANAGEMENT rimaste.

Riapri la app installata sul dispositivo del bambino e segui i passaggi sullo schermo per configurare Bitdefender Parental Control:

1. Tocca **Continua**.
2. Accedi alla app utilizzando le credenziali del tuo account di Bitdefender Central.
3. Seleziona il profilo bambino che vuoi assegnare al dispositivo iOS.
4. Dovrai concedere le autorizzazioni necessarie per la app affinché funzioni correttamente. Tocca **Avanti**.
5. Consenti l'accesso a VPN per filtrare i contenuti online sul dispositivo del bambino. Tocca **Consenti** due volte di fila per aggiungere le configurazioni VPN.
6. Tocca **Avanti**, quindi seleziona **Consenti** per aiutarti a individuare il dispositivo iOS del bambino.
7. Quindi continua la fase di configurazione di Apple Family Control per bloccare l'accesso a Internet e le app sul dispositivo del bambino.

   Attenzione
   Puoi toccare **Scopri come** per una guida passo passo su come farlo.

8. Dopo aver configurato Apple Family Control sul tuo dispositivo e su quello del bambino, seleziona **Ho configurato Apple Family Control** per continuare.
9. Successivamente, consenti l'Accesso al tempo di utilizzo per filtrare i contenuti online sul dispositivo iOS del bambino.
10. Tocca **Termina configurazione**.

.

Dopo aver completato questi passaggi sul dispositivo o sui dispositivi del bambino, il processo di configurazione è completo. In qualità di genitore, ora puoi monitorare le attività online del bambino e visualizzare le statistiche di utilizzo nel tuo account di Bitdefender Central, all'interno della dashboard di Parental Control, che descriveremo in dettaglio nei capitoli successivi.

2. FUNZIONALITÀ E CARATTERISTICHE

2.1. Profili

Un profilo bambino è un insieme personalizzato di regole che consentono alla app Bitdefender Parental Control di gestire e monitorare le attività online di un bambino. Include impostazioni personalizzate in base all'età del bambino, come filtri dei contenuti e restrizioni di tempo. Utilizzando l'account Bitdefender Central, i genitori possono creare, modificare ed eliminare questi profili, nonché assegnare e rimuovere i dispositivi, garantendo un'esperienza online sicura e appropriata per i propri figli.

Per creare un profilo bambino:

1. Vai in Bitdefender Central e accedi al tuo account.
2. Nel menu sul lato sinistro, clicca sulla scheda **Parental Control**.
3. Clicca su **Nuovo profilo** per creare un nuovo profilo bambino.
4. Inserisci i dettagli del bambino, il nome, l'immagine del profilo e la data di nascita.

   > **Attenzione**
   > In base all'età del bambino, Bitdefender blocca automaticamente alcune categorie come chat, social network, contenuti espliciti e altro ancora. Puoi modificare le categorie bloccate in un secondo momento.

5. Clicca sul pulsante **Salva**.

Ora il nuovo profilo è stato creato e verrà visualizzato nella pagina.

Per modificare un profilo bambino:

1. Clicca sul pulsante **Vedi dettagli** dal profilo del bambino.
2. Per modificare il profilo del bambino, vai in **Modifica profilo**.
3. Usa il campo corrispondente per modificare il nome, la data di nascita e/o l'immagine del profilo del bambino.
4. Clicca su **Salva modifiche** dopo aver modificato i dettagli necessari.

Per eliminare un profilo bambino:

1. Clicca sul pulsante **Vedi dettagli** dal profilo del bambino.
2. Vai in **Modifica profilo**.
3. Clicca sul pulsante **Elimina profilo** e conferma l'eliminazione.

Per assegnare i dispositivi a un Profilo bambino:

Se il bambino ha più dispositivi (Windows, macOS, Android o iOS), puoi assegnarli allo stesso profilo bambino.

1. Clicca sul pulsante **Vedi dettagli** dal profilo del bambino.
2. Clicca sul numero di dispositivi elencati sotto il suo nome.
3. Clicca sul pulsante **Assegna dispositivi**.
4. Seleziona il nome del dispositivo, quindi clicca sul pulsante **Assegna**.

> **Attenzione**
> Se il dispositivo non è visibile nell'elenco, clicca su **Installa un nuovo dispositivo**, quindi segui le istruzioni sullo schermo per installare e configurare Bitdefender Parental Control sul nuovo dispositivo.

Per rimuovere i dispositivi da un profilo bambino:

Rimuovendo un dispositivo da un profilo del bambino, significa che il dispositivo non sarà più sotto la gestione di Bitdefender Parental Control. Le regole e le impostazioni specificate nel profilo del bambino non si applicheranno più a quel dispositivo. Anche se la app Parental Control resta installata sul dispositivo, cessa comunque di funzionare.

1. Clicca sul pulsante **Vedi dettagli** dal profilo del bambino.
2. Clicca sul numero di dispositivi elencati sotto il suo nome.
3. Localizza il dispositivo del bambino e clicca sull'opzione **Annulla assegnazione dispositivo**.
4. Premi il pulsante **Sì, annulla assegnazione dispositivo** per confermare l'azione.

2.2. Statistiche

Parental Control fornisce informazioni su come i bambini utilizzano Internet e i propri dispositivi. In questa guida, approfondiremo le varie statistiche disponibili per i genitori in Bitdefender Central,

che consentiranno loro di prendere decisioni informate e garantire un'esperienza online sicura ed equilibrata per i propri bambini.

Per visualizzare le statistiche:

1. Vai in Bitdefender Central e accedi al tuo account.
2. Una volta eseguito l'accesso, clicca sulla scheda **Parental Control** nel menu a sinistra.
3. Clicca sul profilo del bambino di cui si desidera visualizzare le statistiche.

Dopo aver selezionato il profilo del bambino, si aprirà una dashboard che mostra diversi pannelli statistici. Tutti fanno riferimento alle altre funzionalità descritte più avanti in questa documentazione.

2.3. Codice PIN parentale

Il codice PIN parentale è una funzione di sicurezza all'interno della dashboard di Parental Control della piattaforma Bitdefender Central. Serve ai genitori per mantenere il controllo sull'accesso dei propri bambini alla app Bitdefender Parental Control installata sui loro dispositivi. Di seguito è riportata una guida dettagliata su come impostare, trovare e gestire il proprio PIN parentale.

Il codice PIN parentale impedisce la disconnessione non autorizzata dalla app Bitdefender Parental Control sul dispositivo del bambino. Quando il bambino tenta di disconnettersi, gli verrà chiesto di inserire tale codice PIN. Si tratta di un'opzione per garantire che solo tu, in qualità di genitore con accesso all'account di Bitdefender Central, possa controllare le impostazioni della app.

> **Attenzione**
> Quando configuri la app Parental Control per la prima volta, ti sarà chiesto di stabilire un codice PIN parentale di 4-8 cifre.

2.3.1. Hai dimenticato il codice PIN?

Nel caso dimenticassi il tuo codice PIN parentale, puoi recuperarlo facilmente dal tuo account di Bitdefender Central:

1. Vai in Bitdefender Central e accedi al tuo account.

2. Una volta eseguito l'accesso, clicca sulla scheda **Parental Control** nel menu a sinistra.
3. Nell'angolo in alto a destra della pagina, clicca su **Codice PIN**.
4. Clicca sull'icona a forma di occhio per trovare il codice PIN parentale.

2.3.2. Modificare il tuo codice PIN

Se sospetti che il tuo codice PIN sia stato compromesso o semplicemente vuoi aggiornarlo per motivi di sicurezza:

1. Nella sezione di Parental Control del tuo account di Bitdefender Central, clicca sull'opzione **Codice PIN**.
2. Scegli l'opzione **Cambia PIN** e segui le istruzioni sullo schermo per configurare un nuovo codice PIN.

2.4. Filtro contenuti

Il filtro dei contenuti consente ai genitori di limitare l'accesso ai propri bambini a contenuti online, in modo da bloccare intere categorie di siti web o apportare delle eccezioni in base a URL o argomenti specifici.

> **Attenzione**
> La funzionalità di filtro dei contenuti di Bitdefender Parental Control non impedisce al bambino di utilizzare le applicazioni dei siti web offline, poiché gestisce il traffico Internet online dei dispositivi che utilizza.

Per accedere al filtro contenuti:

1. Accedi al tuo account di Bitdefender Central.
2. Nel menu sul lato sinistro, clicca sulla scheda **Parental Control**.
3. Vai al profilo del bambino e clicca sul menu **Altro** in alto a destra. Quindi, seleziona **Filtro contenuti**.

2.4.1. Ricerca sicura e restrizioni di YouTube

Nella sezione **Privacy e Sicurezza** sul lato destro dello schermo, puoi attivare gli interruttori Ricerca sicura e YouTube con restrizioni.

- **Ricerca sicura:** quando si utilizzano i motori di ricerca, Ricerca sicura impedisce la visualizzazione di contenuti ritenuti non sicuri da Google nei risultati della ricerca.
- **YouTube con restrizioni:** fornisce al bambino video adatti alla sua età su YouTube.

> **Attenzione**
> **Ricerca sicura** e **YouTube con restrizioni** reindirizzano tutte le richieste DNS da **google.com** a **safe.google.com**. L'attuale filtraggio dei contenuti viene eseguito da Google. Bitdefender Parental Control non filtra i contenuti all'interno di Ricerca Sicura o Google. Allo stesso modo, YouTube potrebbe non controllare efficacemente i tag sui video, esponendo potenzialmente i bambini a contenuti inappropriati.

2.4.2. Blocco e autorizzazione delle categorie di siti web

> **Attenzione**
> Nella sezione **Categorie**, i tipi di siti web che il bambino può visualizzare online sono consentiti o bloccati per impostazione predefinita, a seconda dell'età impostata al momento della creazione del profilo del bambino.

Puoi bloccare o consentire vari tipi di siti web in qualsiasi momento:

1. Seleziona una categoria.
2. Per bloccare l'accesso a tale categoria, scegli **Bloccata** dal menu a discesa. Per consentire l'accesso, seleziona **Consentita**.

> **Importante**
> Se blocchi la categoria **Condivisione file** per il profilo del bambino, l'aggiornamento di macOS non funzionerà. Ti consigliamo di consentire temporaneamente la condivisione di file durante l'aggiornamento di macOS.

2.4.3. Eccezioni

Nella scheda **Eccezioni**, è possibile impostare le eccezioni di siti web e applicazioni:

- **Eccezioni per sito web:**
  1. Clicca sul pulsante **Aggiungi eccezione**.

2. Seleziona **Solo sito web** e poi clicca sul pulsante **Avanti**.
3. Digita l'indirizzo del sito web e seleziona se consentirlo o bloccarlo dal menu a discesa.
4. Poi clicca sul pulsante **Aggiungi**.

- Eccezioni per app e piattaforme web
  1. Clicca sul pulsante **Aggiungi eccezione**.
  2. Seleziona **App e piattaforma web** e quindi clicca sul pulsante **Avanti**.
  3. Seleziona la piattaforma per la quale desideri fare un'eccezione dall'elenco fornito. In alternativa, usa la barra di ricerca per trovare ciò che stai cercando.
  4. Poi clicca sul pulsante **Aggiungi**.

- **Rimuovi eccezioni:**
  Tutte le eccezioni configurate verranno visualizzate nel Filtro contenuti all'interno dell'elenco designato nella parte inferiore.
  Per eliminare un'eccezione, clicca semplicemente sull'icona del cestino situata a destra della voce.

2.5. Tempo quotidiano su Internet

Nel tuo account di Bitdefender Central, nella sezione Parental Control, per ogni profilo bambino creato, viene visualizzata una scheda Tempo quotidiano su Internet. Questa scheda mostra il tempo totale che il bambino ha trascorso online su tutti i dispositivi assegnati. Per limitare il tempo online di un bambino:

1. Vai al profilo del bambino e clicca sul pulsante **Imposta limite di tempo** nel pannello **Tempo quotidiano su Internet**. In alternativa, puoi cliccare sul menu **Altro** nell'angolo in alto a destra e selezionare **Tempo quotidiano su Internet**.
2. Clicca sul pulsante **Abilita limite di tempo** per attivare questa funzionalità.

> **Attenzione**
> Per impostazione predefinita, il bambino ha a disposizione 1 ora e 30 minuti di accesso a Internet al giorno. Se il genitore non estende questo limite di tempo, l'accesso a Internet del bambino viene interrotto dopo aver raggiunto il limite di 1 ora e 30 minuti.

Rimuovere il limite di tempo giornaliero:

- Per disattivare la funzionalità Tempo quotidiano su Internet, vai alla dashboard del profilo del bambino, clicca sul pulsante **Modifica tempo** nel pannello **Tempo quotidiano su Internet**, quindi seleziona il pulsante **Pausa** nel pannello **Limite di tempo**.
- Per rimuovere il limite di tempo per un giorno particolare, clicca sul pulsante ⊗ corrispondente a quel giorno della settimana nel pannello **Programma**.

Modificare il limite di tempo:

- Per impostare un diverso limite di tempo per un determinato giorno della settimana, clicca sul nome del giorno nel pannello **Programma**, seleziona il limite desiderato dal menu a discesa e clicca sul pulsante **Salva modifiche**. Puoi selezionare più di un giorno alla volta.

2.5.1. Sistema di ricompense

La funzionalità **Ricompensa** ti consente di premiare o estendere il tempo di utilizzo per il bambino, promuovendo buone abitudini online. Puoi usare il sistema di ricompense in due modi diversi:

- **Ricompensa manuale:**
  1. Raggiungi la sezione Parental Control nel tuo account di Bitdefender Central.
  2. Vai al profilo del bambino e clicca sul pulsante **Ricompensa** nel pannello **Tempo quotidiano su Internet**.
  3. Seleziona la quantità di tempo extra che vuoi aggiungere e conferma cliccando su **Ricompensa**.

- **Richiesta del bambino:**
  Quando il bambino raggiunge il limite quotidiano, può richiedere del tempo aggiuntivo tramite la app Parental Control installata sul proprio dispositivo mobile. In qualità di genitore, riceverai una notifica nel tuo account di Bitdefender Central.

1. Una volta effettuato l'accesso al tuo account di Bitdefender Central, cerca un punto rosso sulla campana delle notifiche nell'angolo in alto a destra dello schermo, che indica una richiesta in sospeso da parte di tuo figlio.
2. Esamina la richiesta e decidi quanto tempo in più concedere.

> **Attenzione**
> I bambini hanno la possibilità di richiedere estensioni del loro tempo quotidiano su Internet solo su dispositivi Android e iOS.

2.6. Disattivare Internet sul dispositivo del bambino

In qualità di genitore, gestire l'utilizzo di Internet da parte del bambino può essere molto importante per il suo benessere e la sua produttività. Per disattivare temporaneamente l'accesso a Internet sul dispositivo del bambino utilizzando Bitdefender Parental Control:

1. Vai in Bitdefender Central e accedi al tuo account.
2. Una volta eseguito l'accesso, clicca sulla scheda **Parental Control** nel menu a sinistra.
3. Seleziona **Mostra dettagli** dal profilo del bambino di cui desideri disattivare Internet.
4. Clicca sul pulsante **Blocca Internet** nell'angolo in alto a destra della dashboard del bambino.

> **Attenzione**
> Internet sarà interrotto su tutti i dispositivi del bambino. Questa azione sostituisce tutte le precedenti impostazioni di Parental Control esistenti, ad esempio, le routine, il limite di tempo giornaliero o le categorie consentite.

5. Quando l'accesso a Internet viene interrotto, il pulsante **Blocca Internet** viene modificato in **Riprendi Internet**. Per ripristinare l'accesso a Internet, clicca sul pulsante **Riprendi Internet**.

2.7. Routine

In Bitdefender Parental Control puoi impostare fino a 3 routine distinte per programmare la disattivazione dell'accesso a Internet. Forniscono un approccio strutturato alla gestione delle attività online di un

bambino, promuovendo le buone abitudini e il coinvolgimento della famiglia, garantendo al contempo la sua sicurezza. Queste routine sono indipendenti l'una dall'altra, il che significa che puoi scegliere di attivarne solo una, due o tutte e tre in base alle tue preferenze:

- **Tempo per lo studio**
  Crea un programma che includa tempo per i compiti, lo studio e altre attività.
- **Ore notturne**
  Usa la routine Periodo di riposo per escludere un periodo di riposo per il bambino.
- **Tempo in famiglia**
  Usa la routine Tempo in famiglia per escludere il tempo in cui il bambino è presente durante i pasti in famiglia, ad esempio.

> **Attenzione**
> **Routine rispetto al Tempo quotidiano su Internet:**
>
> Durante le routine, il tempo trascorso online non viene conteggiato ai fini del limite di tempo quotidiano su Internet. Una volta terminata la routine, la funzione Tempo quotidiano su Internet riprende a conteggiare l'utilizzo di Internet da parte del bambino.
>
> Per evitare confusione per i genitori, mentre è in corso una routine, la scheda Tempo quotidiano su Internet non sarà visibile nella dashboard del profilo del bambino fino al termine della routine. Invece, durante questo periodo, verrà visualizzato il nome della routine attiva.

2.7.1. Impostare le routine

Per impostare una delle routine di Parental Control:

1. Vai in Bitdefender Central e accedi al tuo account.
2. Nel menu sul lato sinistro, clicca sulla scheda **Parental Control**.
3. Vai al profilo del bambino e seleziona la routine desiderata dal menu **Altro**.
4. Clicca sul pulsante **Attiva** per attivare la routine selezionata.
5. Verranno visualizzati i pannelli **Programma** e **Accesso a Internet**.
   - **Programma:**
     Per impostare una routine per uno o più giorni della settimana:

a. Seleziona i giorni desiderati.

b. Seleziona l'ora di inizio e di fine della routine dal menu a discesa fornito.

c. Infine, clicca sul pulsante **Salva modifiche** per confermare le tue scelte.

Per rimuovere la routine per un determinato giorno, clicca sul pulsante ⊗ corrispondente a quel giorno della settimana.

- **Accesso a Internet:**
  Il pannello di accesso a Internet all'interno di una routine offre due funzioni principali per controllare le attività del bambino durante intervalli di tempo specifici:

  - **Interruzione completa di Internet:** i genitori hanno la possibilità di disattivare completamente l'accesso a Internet per il bambino durante l'orario di routine programmato. Disattivando l'interruttore di **accesso a Internet**, i dispositivi del bambino non saranno in grado di accedere a Internet nel periodo di tempo designato.

  - **Categoria o sito web selettivo:** in alternativa, i genitori possono scegliere di consentire l'accesso a Internet durante le ore della routine, ma limitare determinati siti web o categorie di contenuti. Attivando l'interruttore di **accesso a Internet**, diventano visibili due schede aggiuntive, ovvero le schede **Categorie** ed **Eccezioni**, che consentono di accedere a ulteriori impostazioni di filtro dei contenuti</link>. (pagina 12)

2.8. Tracciamento della posizione del bambino

Con la diffusione sempre maggiore di smartphone e altri dispositivi mobili, il tracciamento della posizione del bambino è diventato essenziale per molte famiglie. Che si tratti di sapere dove si trova dopo la scuola o durante le uscite con gli amici, avere la possibilità di monitorare la sua posizione offre maggiore tranquillità ai genitori. Ecco una guida passo passo su come tracciare la posizione del bambino usando la funzione Posizione di Bitdefender Parental Control.

1. Vai in Bitdefender Central e accedi al tuo account.

2. Una volta eseguito l'accesso, clicca sulla scheda **Parental Control** nel menu a sinistra.
3. Se hai più bambini, seleziona **Mostra dettagli** dal profilo del bambino di cui desideri monitorare la posizione.
4. Nel pannello Posizione, seleziona il dispositivo Android o iOS che vuoi monitorare, clicca sul pulsante **Localizza**.

> **Attenzione**
> La funzionalità Posizione in Bitdefender Parental Control non è disponibile per i dispositivi Windows e macOS.

5. Dopo una breve attesa, un perno rosso indicherà la posizione attuale del bambino sulla mappa.

> **Attenzione**
> Gli aggiornamenti della posizione si verificano ogni 20 minuti. Se tenti di rintracciare la posizione del bambino in meno di 20 minuti dalla posizione precedente, la posizione visualizzata potrebbe non riflettere la sua posizione reale.

3. DISINSTALLARE PARENTAL CONTROL

Disinstallare Bitdefender Parental Control sui dispositivi Windows:

1. Rimuovi il dispositivo dal profilo del bambino in Bitdefender Central.
2. Apri il Pannello di Controllo sul dispositivo in questione e localizza Bitdefender Parental Control nell'elenco **Programmi e funzionalità**.
3. Disinstalla Bitdefender Parental Control.

Disinstallare Bitdefender Parental Control sui dispositivi macOS:

1. Rimuovi il dispositivo dal profilo del bambino in Bitdefender Central.
2. Apri il **Finder** sul dispositivo macOS.
3. Accedi alle tue Applicazioni e localizza la cartella Bitdefender.
4. Aprila ed esegui **Bitdefender Uninstaller**.
5. Scegli Bitdefender Parental Control dall'elenco di prodotti da disinstallare.
6. Fornisci le credenziali di amministratore e attendi il completamento della disinstallazione.

Disinstallare Bitdefender Parental Control sui dispositivi Android e iOS:

1. Rimuovi il dispositivo dal profilo del bambino in Bitdefender Central.
2. Disinstalla Parental Control dal dispositivo mobile come qualsiasi altra applicazione o rispettivamente tramite Google Play Store o App Store.

4. OTTENERE AIUTO

4.1. Richiesta d'aiuto

Bitdefender offre ai suoi clienti un livello impareggiabile di supporto rapido e accurato. Se dovessi riscontrare un qualche problema o se avessi domande sul tuo prodotto Bitdefender, potrai usare diverse risorse online per trovare una soluzione o una risposta. Allo stesso tempo, potrai contattare il servizio clienti di Bitdefender. I nostri responsabili del supporto risponderanno alle tue domande in maniera tempestiva e ti forniranno tutto l'aiuto necessario.

4.2. Risorse online

Sono disponibili diverse risorse online per aiutarti a risolvere i tuoi problemi e le tue domande relative a Bitdefender.

- Centro di supporto di Bitdefender:
  https://www.bitdefender.it/consumer/support/
- La community di esperti di Bitdefender:
  https://community.bitdefender.com/en/
- Bitdefender Cyberpedia:
  https://www.bitdefender.com/cyberpedia/

Puoi anche usare il tuo motore di ricerca preferito per trovare più informazioni sulla sicurezza del computer, i prodotti Bitdefender e la società.

4.2.1. Centro di supporto di Bitdefender

Il Centro di supporto di Bitdefender è un archivio online di informazioni sui prodotti Bitdefender. Conserva, in un formato facilmente accessibile, le notifiche sui risultati delle attività di risoluzioni bug e problemi del supporto tecnico di Bitdefender e dei team di sviluppo, oltre ad articoli più generali sulla prevenzione delle minacce, la gestione delle soluzioni di Bitdefender con spiegazioni dettagliate e molti altri articoli.

Il Centro di supporto di Bitdefender è aperto al pubblico e gratuitamente esplorabile. Le ricche informazioni che contiene sono un altro modo per fornire ai clienti di Bitdefender le conoscenze tecnologiche e le

informazioni necessarie. Tutte le richieste di informazioni o i rapporti sui difetti, provenienti dai clienti di Bitdefender, prima o poi arrivano al Centro di supporto di Bitdefender, come rapporti di disinfezione, metodi per aggirare le truffe, o articoli informativi, per integrare i file di aiuto dei prodotti.

Il Centro assistenza di Bitdefender è disponibile in qualsiasi momento al seguente indirizzo: https://www.bitdefender.it/consumer/support/.

4.2.2. La community di esperti di Bitdefender

La community di esperti è un ambiente in cui gli utenti di Bitdefender, oltre a fan e appassionati, possono interagire, scambiare idee, supportarsi a vicenda e condividere le proprie conoscenze e soluzioni. È anche un luogo creativo e fornisce feedback preziosi ai nostri team di sviluppo. I membri della community sono utenti esperti di Bitdefender, felici di aiutare altri utenti nel proprio tempo libero. Grazie al loro immenso contributo e sforzi volontari, abbiamo creato una knowledge base dove gli utenti possono trovare risposte e aiuto, ma con un tocco più umano di una semplice risposta automatizzata.

Qui potrai trovare molte conversazioni utili con utenti che utilizzano Bitdefender sui propri dispositivi. La community offre una vera connessione con i nostri membri e fa sentire la loro voce. Ti invitiamo a parteciparvi sapendo che la tua opinione e le tue informazioni saranno rispettate e apprezzate. In qualità di fornitore stimato, ci sforziamo di offrire un livello senza precedenti di supporto sempre rapido e preciso, sperando di avvicinare sempre più i nostri utenti. Abbiamo progettato la nostra community con questo obiettivo sempre in mente.

Puoi trovare la pagina web della nostra community di esperti qui:

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

4.2.3. Bitdefender Cyberpedia

Bitdefender Cyberpedia include tutte le informazioni necessarie sulle minacce informatiche più recenti. È anche dove gli esperti Bitdefender condividono trucchi e suggerimenti su come restare protetti da hacker, violazioni, furti d'identità e tentativi d'impersonificazione dei social.

La pagina web di Bitdefender Cyberpedia è disponibile qui:

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

4.3. Informazioni di contatto

Una comunicazione efficiente è la chiave per un business di successo. Dal 2001 BITDEFENDER ha stabilito una reputazione indiscutibile impegnandosi costantemente per una migliore comunicazione in modo da superare le aspettative dei nostri clienti e partner. In caso di domande, non esitate a contattarci direttamente tramite il ns Centro di supporto di Bitdefender (pagina 21).

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

4.3.1. Distributori locali

I distributori locali di Bitdefender sono pronti a rispondere a ogni richiesta inerente le loro zone operative, sia in ambito commerciale sia generale.

Per trovare un distributore di Bitdefender nel tuo paese:

1. Vai a https://www.bitdefender.com/partners/partner-locator.html.
2. Seleziona il tuo paese e la tua città, utilizzando le opzioni corrispondenti.

GLOSSARIO

Codice di attivazione

È una chiave unica che può essere acquistata dal rivenditore e usata per attivare un servizio o un prodotto specifico. Un codice di attivazione consente l'attivazione di un abbonamento valido per un determinato periodo di tempo e un certo numero di dispositivi. Inoltre, può anche essere utilizzato per estendere un abbonamento, a condizione che venga generato per lo stesso prodotto o servizio.

ActiveX

ActiveX è un modello per la scrittura di programmi in modo che altri programmi e il sistema operativo possano chiamarli. La tecnologia ActiveX viene utilizzata con Microsoft Internet Explorer per creare pagine Web interattive che sembrano e si comportano come programmi per computer, piuttosto che come pagine statiche. Con ActiveX, gli utenti possono porre o rispondere a domande, utilizzare pulsanti e interagire in altri modi con la pagina web. I controlli ActiveX vengono spesso scritti utilizzando Visual Basic. Active X si distingue per una completa mancanza di controlli di sicurezza; gli esperti di sicurezza informatica ne scoraggiano l'uso su Internet.

Minaccia persistente avanzata

Advanced Persistent Threat (APT) sfrutta le vulnerabilità dei sistemi per rubare informazioni importanti per consegnarle alla fonte. Grandi gruppi come organizzazioni, aziende o governi sono presi di mira da questa minaccia. L'obiettivo di una minaccia persistente avanzata è rimanere inosservato per lungo tempo essendo in grado di monitorare e raccogliere informazioni importanti senza danneggiare le macchine mirate. Il metodo utilizzato per iniettare la minaccia nella rete è attraverso un file PDF o un documento di Office che sembra innocuo in modo che ogni utente possa eseguire i file.

Adware

L'adware è spesso combinato con un'app host fornita gratuitamente a condizione che l'utente accetti l'adware. Poiché le app adware vengono generalmente installate dopo che l'utente ha accettato un contratto di licenza che stabilisce lo scopo dell'app, non viene commesso alcun reato. Tuttavia, le pubblicità pop-up possono diventare fastidiose e in alcuni casi

degradare le prestazioni del sistema. Inoltre, le informazioni raccolte da alcune di queste app possono causare problemi di privacy per gli utenti che non erano pienamente a conoscenza dei termini del contratto di licenza.

Archivio

Un disco, un nastro o una cartella che contiene file memorizzati.

Un file che contiene uno o più file in un formato compresso.

Porta sul retro

Un buco nella sicurezza di un sistema deliberatamente lasciato in essere da progettisti o manutentori. La motivazione di tali buchi non è sempre sinistra; alcuni sistemi operativi, ad esempio, escono dalla confezione con account privilegiati destinati all'uso da parte dei tecnici dell'assistenza sul campo o dei programmatori di manutenzione del fornitore.

Settore di avvio

Un settore all'inizio di ogni disco che identifica l'architettura del disco (dimensione del settore, dimensione del cluster e così via). Per i dischi di avvio, il settore di avvio contiene anche un programma che carica il sistema operativo.

Avvio virus

Una minaccia che infetta il settore di avvio di un disco fisso o floppy. Un tentativo di avvio da un dischetto infettato da un virus del settore di avvio causerà l'attivazione della minaccia nella memoria. Ogni volta che avvierai il tuo sistema da quel momento in poi, avrai la minaccia attiva in memoria.

Botnet

Il termine “botnet” è composto dalle parole “robot” e “network”. Le botnet sono dispositivi connessi a Internet infettati da minacce e possono essere utilizzati per inviare e-mail di spam, rubare dati, controllare da remoto dispositivi vulnerabili o diffondere spyware, ransomware e altri tipi di minacce. Il loro obiettivo è quello di infettare il maggior numero possibile di dispositivi connessi, come PC, server, dispositivi mobili o IoT appartenenti a grandi aziende o industrie.

Navigatore

Abbreviazione di browser Web, un'app software utilizzata per individuare e visualizzare pagine Web. I browser più diffusi includono Microsoft Internet Explorer, Mozilla Firefox e Google Chrome. Questi sono browser

grafici, il che significa che possono visualizzare grafica e testo. Inoltre, la maggior parte dei browser moderni può presentare informazioni multimediali, inclusi audio e video, sebbene richiedano plug-in per alcuni formati.

Attacco di forza bruta

Attacco di indovinazione della password utilizzato per irrompere in un sistema informatico inserendo possibili combinazioni di password, per lo più a partire dalla password più facile da indovinare.

Riga di comando

In un'interfaccia a riga di comando, l'utente digita i comandi nello spazio fornito direttamente sullo schermo utilizzando il linguaggio dei comandi.

Biscotti

Nell'industria di Internet, i cookie sono descritti come piccoli file contenenti informazioni su singoli computer che possono essere analizzati e utilizzati dagli inserzionisti per tenere traccia dei tuoi interessi e gusti online. In questo ambito, la tecnologia dei cookie è ancora in fase di sviluppo e l'intenzione è quella di indirizzare gli annunci direttamente a ciò che hai dichiarato di essere i tuoi interessi. È un'arma a doppio taglio per molte persone perché, da un lato, è efficiente e pertinente in quanto si vedono solo annunci su ciò che ti interessa. cosa clicchi. Comprensibilmente, c'è un dibattito sulla privacy e molte persone si sentono offese dall'idea di essere viste come un "numero SKU" (sai, il codice a barre sul retro dei pacchi che viene scansionato alla cassa della drogheria) . Sebbene questo punto di vista possa essere estremo, in alcuni casi è accurato.

Cyber bullismo

Quando coetanei o estranei commettono atti violenti contro i bambini apposta per ferirli fisicamente. Per danneggiare emotivamente, gli aggressori inviano messaggi meschini o foto poco lusinghiere, isolando così le loro vittime dagli altri o sentendosi frustrate.

Dizionario Attacco

Attacchi di indovinazione della password utilizzati per irrompere in un sistema informatico inserendo una combinazione di parole comuni per generare potenziali password. Lo stesso metodo viene utilizzato per indovinare le chiavi di decrittazione di messaggi o documenti crittografati.

Gli attacchi con dizionario hanno successo perché molte persone tendono a scegliere password brevi e con parole singole facili da indovinare.

Unità disco

È una macchina che legge e scrive dati su un disco. Un disco rigido legge e scrive dischi rigidi. Un'unità floppy accede ai dischi floppy. Le unità disco possono essere interne (alloggiate all'interno di un computer) o esterne (alloggiate in una scatola separata che si collega al computer).

Scaricamento

Per copiare i dati (di solito un intero file) da una fonte principale a un dispositivo periferico. Il termine è spesso usato per descrivere il processo di copia di un file da un servizio online al proprio computer. Il download può anche riferirsi alla copia di un file da un file server di rete a un computer in rete.

E-mail

Mail elettronica. Un servizio che invia messaggi sui computer tramite reti locali o globali.

Eventi

Un'azione o un evento rilevato da un programma. Gli eventi possono essere azioni dell'utente, come fare clic su un pulsante del mouse o premere un tasto, o occorrenze di sistema, come l'esaurimento della memoria.

Exploit

Un modo per sfruttare diversi bug o vulnerabilità presenti in un computer (software o hardware). Pertanto, gli hacker possono ottenere il controllo di computer o reti.

Falso positivo

Si verifica quando uno scanner identifica un file come infetto quando in realtà non lo è.

Estensione del nome file

La parte di un nome di file, dopo il punto finale, che indica il tipo di dati memorizzati nel file. Molti sistemi operativi utilizzano estensioni di file, ad esempio Unix, VMS e MS-DOS. Di solito sono da una a tre lettere (alcuni tristi vecchi sistemi operativi non supportano più di tre). Gli esempi includono "c" per codice sorgente C, "ps" per PostScript, "txt" per testo arbitrario.

Euristico

Un metodo basato su regole per identificare nuove minacce. Questo metodo di scansione non si basa su uno specifico database di informazioni sulle minacce. Il vantaggio della scansione euristica è che non viene ingannata da una nuova variante di una minaccia esistente. Tuttavia, potrebbe occasionalmente segnalare codice sospetto nei normali programmi, generando il cosiddetto "falso positivo".

Vaso di miele

Un sistema informatico esca impostato per attirare gli hacker per studiare il modo in cui agiscono e identificare i metodi eretici che utilizzano per raccogliere informazioni di sistema. Le aziende e le aziende sono più interessate a implementare e utilizzare gli honeypot per migliorare il proprio stato di sicurezza generale.

IP

Protocollo Internet - Un protocollo instradabile nella suite di protocolli TCP/IP responsabile dell'indirizzamento IP, del routing e della frammentazione e riassemblaggio dei pacchetti IP.

Applet Java

Un programma Java progettato per essere eseguito solo su una pagina Web. Per utilizzare un'applet su una pagina Web, devi specificare il nome dell'applet e la dimensione (lunghezza e larghezza, in pixel) che l'applet può utilizzare. Quando si accede alla pagina Web, il browser scarica l'applet da un server e la esegue sulla macchina dell'utente (il client). Le applet differiscono dalle app in quanto sono governate da un rigido protocollo di sicurezza.

Ad esempio, anche se le applet vengono eseguite sul client, non possono leggere o scrivere dati sulla macchina del client. Inoltre, le applet sono ulteriormente limitate in modo che possano solo leggere e scrivere dati dallo stesso dominio da cui sono servite.

Registratore di tasti

Un keylogger è un'app che registra tutto ciò che digiti. I keylogger non sono di natura dannosa. Possono essere utilizzati per scopi legittimi, come il monitoraggio dell'attività dei dipendenti o dei bambini. Tuttavia, vengono sempre più utilizzati dai criminali informatici per scopi dannosi (ad esempio, per raccogliere dati privati, come credenziali di accesso e numeri di previdenza sociale).

Virus a macroistruzione

Un tipo di minaccia informatica codificata come macro incorporata in un documento. Molte app, come Microsoft Word ed Excel, supportano potenti linguaggi macro. Queste app ti consentono di incorporare una macro in un documento e di eseguire la macro ogni volta che il documento viene aperto.

Cliente di posta

Un client di posta elettronica è un'app che consente di inviare e ricevere e-mail.

Memoria

Aree di archiviazione interne nel computer. Il termine memoria identifica l'archiviazione dei dati sotto forma di chip e la parola archiviazione viene utilizzata per la memoria che esiste su nastri o dischi. Ogni computer viene fornito con una certa quantità di memoria fisica, solitamente indicata come memoria principale o RAM.

Non euristico

Questo metodo di scansione si basa su uno specifico database di informazioni sulle minacce. Il vantaggio della scansione non euristica è che non si lascia ingannare da quella che potrebbe sembrare una minaccia e non genera falsi allarmi.

Predatori online

Individui che cercano di attirare minori o adolescenti in conversazioni apposta per coinvolgerli in attività sessuali illegali. I social network sono il luogo ideale in cui i bambini vulnerabili possono essere facilmente cacciati e indotti a commettere attività sessuali, online o faccia a faccia.

Programmi confezionati

Un file in un formato di compressione. Molti sistemi operativi e app contengono comandi che consentono di comprimere un file in modo che occupi meno memoria. Ad esempio, supponi di avere un file di testo contenente dieci caratteri spazio consecutivi. Normalmente, ciò richiederebbe dieci byte di archiviazione.

Tuttavia, un programma che comprime i file sostituirà i caratteri di spazio con uno speciale carattere di serie di spazi seguito dal numero di spazi da sostituire. In questo caso, i dieci spazi richiederebbero solo due byte. Questa è solo una delle tecniche di confezionamento, ce ne sono molte altre.

Sentiero

Le indicazioni esatte per un file su un computer. Queste direzioni sono solitamente descritte per mezzo del sistema di archiviazione gerarchico dall'alto verso il basso.

Il percorso tra due punti qualsiasi, ad esempio il canale di comunicazione tra due computer.

Phishing

L'atto di inviare un'e-mail a un utente che afferma falsamente di essere un'impresa legittima e consolidata nel tentativo di indurre l'utente a cedere informazioni private che verranno utilizzate per il furto di identità. L'e-mail indirizza l'utente a visitare un sito Web in cui viene chiesto di aggiornare le informazioni personali, come password e numeri di carta di credito, previdenza sociale e conto bancario, che l'organizzazione legittima già possiede. Il sito Web, tuttavia, è fasullo e impostato solo per rubare le informazioni dell'utente.

Fotone

Photon è una tecnologia di Bitdefender innovativa e discreta, progettata per minimizzare l'impatto della tua soluzione di sicurezza sulle prestazioni del sistema. Monitorando in background l'attività del PC, crea degli schemi di utilizzo, per ottimizzare i processi di avvio e scansione.

Virus polimorfo

Una minaccia che modifica la propria forma con ogni file che infetta. Non avendo caratteristiche binarie costanti, queste minacce sono difficili da identificare.

Porta

Un'interfaccia su un computer alla quale puoi connettere un supporto. I PC hanno vari tipi di porte. Internamente ci sono varie porte per la connessione di unità disco, schermi e tastiere. Esternamente hanno porte per la connessione di modem, stampanti, mouse e altre periferiche.

Nelle reti TCP/IP e UDP, un endpoint per una connessione logica. Il numero della porta identifica di che tipo di porta si tratta. Ad esempio, la porta 80 viene usata per il traffico HTTP.

Ransomware

Un ransomware è un programma dannoso che prova a sottrarre illecitamente denaro agli utenti bloccando i loro sistemi vulnerabili.

CryptoLocker, CryptoWall e TeslaWall sono solo alcune delle varianti che cercano di bloccare i sistemi personali degli utenti.

L'infezione può partire, aprendo e-mail di spam, scaricando gli allegati di un messaggio o installando determinate applicazioni, il tutto lasciando l'utente ignaro di ciò che sta accadendo sul suo sistema. Gli autori di ransomware puntano a colpire soprattutto gli utenti normali e le aziende.

File di rapporto

File che elenca le azioni avvenute. Bitdefender mantiene un file di rapporto che elenca i percorsi esaminati, le cartelle, il numero di archivi e i file esaminati, oltre a quanti file infetti e sospetti sono stati trovati.

Rootkit

Un rootkit è una serie di strumenti software che offre accesso a livello di amministratore a un sistema. Il termine fu usato per la prima volta per i sistemi operativi UNIX e faceva riferimento a strumenti ricompilati che fornivano agli intrusi i diritti di amministratore, consentendo loro di celare la propria presenza in modo da non dover essere visti dai veri amministratori del sistema.

Il ruolo principale dei rootkit è nascondere i processi, i file, i login e i log. Possono anche intercettare dati dai terminali, dalle connessioni di rete o dalle periferiche, se incorporano il software adeguato.

I rootkit non sono dannosi per natura. Ad esempio, i sistemi e persino alcune applicazioni nascondono file critici utilizzando i rootkit. Comunque, vengono principalmente utilizzati per nascondere minacce o per celare la presenza di un intruso nel sistema. Se combinati alle minacce, i rootkit rappresentano una grave minaccia per l'integrità e la sicurezza di un sistema. Possono monitorare il traffico, creare backdoor nel sistema, alterare file e registri, ed evitare il rilevamento.

Script

Altro termine per macro o file batch, uno script è una lista di comandi che possono essere eseguiti senza interazione con l'utente.

Spam

Messaggi di posta elettronica o newsgroup indesiderati. Generalmente conosciuti come e-mail non desiderate.

Spyware

Qualsiasi software che raccoglie segretamente informazioni dell'utente tramite la sua connessione a Internet, senza che questo se ne accorga, di solito per scopi pubblicitari. Le applicazioni spyware in genere sono incluse come componente nascosta di programmi freeware o shareware, che possono essere scaricati da Internet. Tuttavia, occorre segnalare che la maggioranza delle applicazioni shareware o freeware non includono alcun programma spyware. Una volta installato, uno spyware monitora le attività dell'utente su Internet e trasmette di nascosto tali informazioni a qualcun altro. Gli spyware possono anche raccogliere informazioni su indirizzi e-mail o addirittura password e numeri di carta di credito.

Gli spyware sono simili a un Trojan che gli utenti installano inconsapevolmente installando altre applicazioni. Un modo comune per diventare vittima degli spyware è utilizzare i programmi peer-to-peer attuali per condividere e scaricare file.

Oltre a questioni di etica e privacy, gli spyware sottraggono risorse di memoria al computer, "mangiandosi" larghezza di banda poiché inviano informazioni alla propria "base" usando la connessione internet dell'utente. Poiché gli spyware utilizzano memoria e risorse del sistema, le applicazioni eseguite in background possono provocare instabilità o blocchi del sistema.

Articoli di avvio

Qualsiasi file posizionato in questa cartella si aprirà all'avvio del computer. Ad esempio, una schermata di avvio, un file audio da eseguire quando il computer si avvia la prima volta, una agenda-calendario, oppure app che possono essere elementi di avvio. Normalmente in questa cartella viene posizionato un alias di un file, al posto del file stesso.

Abbonamento

Un accordo di acquisto che offre all'utente il diritto di utilizzare un particolare prodotto o servizio su un numero specifico di dispositivi e per un certo periodo di tempo. Un abbonamento scaduto può essere rinnovato automaticamente, utilizzando le informazioni fornite dall'utente con il primo acquisto.

Area di notifica

Introdotta con Windows 95, la barra degli strumenti è situata nella barra delle applicazioni di Windows (in genere in basso vicino all'orologio) e contiene icone miniaturizzate per un accesso veloce a funzioni di sistema come fax, stampante, modem, volume e molto altro. Clicca due volte o

clicca con il pulsante destro su un'icona per visualizzare e accedere a dettagli e controlli.

TCP/IP

Transmission Control Protocol/Internet Protocol – Insieme di protocolli di rete largamente utilizzati su Internet, che consentono le comunicazioni attraverso le reti interconnesse di computer con diverse architetture hardware e vari sistemi operativi. TCP/IP include gli standard su come comunicano i computer e le convenzioni per connettere le reti e il relativo traffico.

Minaccia

Un programma o parte di codice caricato sul computer a propria insaputa e che viene eseguito contro la propria volontà. La maggior parte delle minacce è anche in grado di auto replicarsi. Tutte le minacce informatiche sono state create dall'uomo. È relativamente facile produrre una semplice minaccia in grado di copiare sé stessa innumerevoli volte. Persino una minaccia così semplice è pericolosa in quanto utilizzerà velocemente tutta la memoria disponibile e porterà il sistema allo stallo. Un tipo di minaccia ancora più pericolosa è quella in grado di trasmettere sé stessa attraverso le reti superando i sistemi di sicurezza.

Aggiornamento delle informazioni sulle minacce

Lo schema binario di una minaccia, usato dalla soluzione di sicurezza per rilevare ed eliminare la minaccia.

Troiano

Un programma distruttivo che si maschera da applicazione benevola. A differenza di programmi software dannosi e worm, i trojan non si replicano ma possono essere altrettanto distruttivi. Un tipo di minaccia Trojan particolarmente insidiosa è un programma che dichiara di pulire le minacce dal computer, ma al contrario le introduce.

Il termine deriva dalla storia dell'Iliade di Omero, dove i Greci mandarono un gigantesco cavallo di legno ai loro avversari, i Troiani, apparentemente come offerta di pace. Ma dopo che i Troiani portarono il cavallo all'interno delle mura della loro città, durante la notte, i soldati Greci uscirono dal ventre cavo del cavallo e aprirono le porte della città, consentendo ai loro compatrioti di entrare e conquistare Troia.

Aggiornamento

Una nuova versione di un prodotto software o hardware creato per sostituire una versione precedente dello stesso prodotto. In aggiunta, le routine di installazione degli aggiornamenti spesso verificano e si assicurano che sia già installata una versione precedente sul computer; diversamente non sarà possibile installare l'aggiornamento.

Bitdefender dispone della propria funzionalità di aggiornamento, che consente la verifica manuale degli aggiornamenti, oppure l'aggiornamento automatico del prodotto.

Virtual Private Network (VPN)

È una tecnologia che consente una connessione diretta temporanea e cifrata a una determinata rete su una rete meno sicura. In questo modo, la ricezione e l'invio dei dati sono sempre sicuri e cifrati, ma soprattutto più difficili da intercettare dai pirati informatici. Una prova di sicurezza è l'autenticazione, che può essere fatta solo usando un nome utente e una password.

Verme

Programma che si propaga in una rete, riproducendosi durante lo spostamento. Non si può attaccare ad altri programmi.