MANUALE D'USO

Bitdefender CONSUMER SOLUTIONS

Digital Identity Protection

Bitdefender Digital Identity Protection

Guida dell'utente

Data di pubblicazione 06/09/2023

Avviso legale

Bitdefender

Indice

INFORMAZIONI SU QUESTA GUIDA

Finalità e destinatari

Questo Bitdefender Digital Identity Protectionmanuale è rivolto a tutti gli utenti che hanno scelto Bitdefender Digital Identity Protection come proprio strumento software dedicato per restare al sicuro dalla crescente ondata di violazioni dei dati online. È una guida accessibile e consultabile da tutti, non solo agli esperti di computer.

Scoprirai come iniziare a prendere il controllo della tua privacy online consentendo a Bitdefender Digital Identity Protection di esaminare il web per fughe non autorizzate dei tuoi dati personali, monitorando se i tuoi account sono stati esposti e semplificando la possibilità di intraprendere azioni prima che si verifichino danni. Apprenderai come ottenere il meglio da Bitdefender.

Buona lettura e speriamo che lo troverai utile.

Come usare questo manuale

Questo manuale presenta alcuni argomenti principali:

Come iniziare (pagina 6)

Inizia a usare Bitdefender Digital Identity Protection e la sua interfaccia utente.

Violazioni dei dati (pagina 11)

Scopri come prenderti cura della protezione della tua identità digitale. Inizia comprendendo cosa sono le violazioni dei dati e come verificarle così da intraprendere le azioni corrette per la protezione della tua privacy online.

Ottenere aiuto (pagina 17)

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. COS'È BITDEFENDER DIGITAL IDENTITY PROTECTION

Oggigiorno la sicurezza e la privacy online sono solo alcuni degli obiettivi principali degli utenti di Internet. E ci sono alcune ottime ragioni. Con gravi violazioni dei dati che si verificano il più delle volte, è assolutamente fondamentale assicurarsi che le tue informazioni di identificazione personale (PII) sia al sicuro e protette.

Ma cosa può essere classificato come informazione di identificazione personale? Tradizionalmente, informazioni sensibili come il nome completo, il codice fiscale, il numero della patente, l'indirizzo e-mail o i dati della carta di credito erano considerate PII. In seguito, anche informazioni meno sensibili, come i codici postali, gli indirizzi IP o gli ID di accesso sono state incluse in questa categoria. Col tempo, la tua traccia digitale, ovvero i dati che ti lasci alle spalle come risultato della tua navigazione Internet, potrebbe arrivare a includere alcuni di questi dati.

Bitdefender Digital Identity Protection rappresenta una vita privata per la libertà online, consentendoti di riottenere il controllo della tua vita digitale. E richiede solo il tuo nome, l'indirizzo e-mail più usato e il tuo numero di telefono. In base a questi dati, cerca sia sul web ufficiale che sul dark web le informazioni personali che sono state esposte pubblicamente.

Bitdefender Digital Identity Protection offre i seguenti:

- **Servizi di monitoraggio e rilevamento:** monitora più di 100 informazioni di identificazione personale come codici fiscali, numeri di carta di credito o indirizzi domestici, e mostra tutti i dati trovati sulla tua traccia online.

  > **Nota**
  > Bitdefender non memorizza o elabora informazioni di identificazione personale. Vengono conservati solo i riferimenti di potenziali violazioni dei dati senza includere dati sensibili.

- **Allerte in tempo reale:** ricevi notifiche su violazioni dei dati e dati esposti nel dark web, informazioni personali nel web ufficiale e potenziali impersonificatori sui social media.
- **Soluzioni:** i nostri servizi suggeriscono azioni chiare necessarie per risolvere i problemi e forniscono promemoria se un problema non

viene risolto completamente. Possono fornire anche istruzioni su come rimuovere annunci personalizzati, esportare i tuoi dati o disattivare la tracciatura.

2. COME INIZIARE

2.1. Attivare Digital Identity Protection

Attiva l'abbonamento a Bitdefender Digital Identity Protection una volta effettuato e pagato il tuo ordine.

1. Apri l'e-mail di conferma ricevuta subito dopo aver completato il tuo ordine e clicca su **COME INIZIARE**.
2. Passerai alla pagina https://central.bitdefender.com.
   Accedi con il tuo account di Bitdefender Central. Se non ne hai uno, scegli di crearlo.
3. Dopo aver effettuato l'accesso, l'abbonamento sarà collegato automaticamente al tuo account di Central e inizierà la fase di introduzione.

In alternativa:

- accedi al pannello **I miei abbonamenti** da Central, localizzato sul lato sinistro della finestra e clicca su **+ Attiva con codice**.
- digita il codice a 10 cifre trovato nell'e-mail di conferma e premi **ATTIVA**.
- se richiesto, seleziona come usare il codice e clicca su **ATTIVA**.

2.2. Configurare Digital Identity Protection

1. Vai in https://central.bitdefender.com/ e accedi al tuo account.
   Se non hai già un account, seleziona **CREA ACCOUNT** e inserisci il tuo nome completo, un indirizzo e-mail e una password.
2. Seleziona il pannello Digital Identity Protection.
   Comparirà una schermata di benvenuto.
3. Clicca su **INIZIA**.
4. Ora ti saranno illustrate le informazioni che devi fornire. I tuoi dati saranno sempre cifrati e protetti.
   Clicca su **AVANTI**.
5. Inserisci il tuo nome, secondo nome (se ne hai uno) e cognome negli spazi corrispondenti, poi clicca su **AVANTI**.

6. Inserisci il tuo indirizzo e-mail e clicca su **AVANTI**.
   Assicurati che sia un indirizzo e-mail valido a cui puoi accedere.
7. Un codice di sicurezza viene inviato all'indirizzo che hai fornito.
   Apri il messaggio, copia il codice e incollalo nello spazio corrispondente.
   Poi, clicca su **VERIFICA**.
8. Seleziona il paese e inserisci il tuo numero di telefono, poi clicca su **AVANTI**.
9. Poco dopo dovresti ricevere un codice di sicurezza.
   Inserisci il codice e seleziona **VERIFICA**.
10. Una volta eseguita la verifica iniziale, clicca su **TERMINA**.

.

> **Nota**
> Riceverai una notifica se durante il primo controllo venisse rilevata una qualsiasi vuolazione, oltre a informazioni di identificazione personale o potenziali impersonificazioni.

Ora Bitdefender Digital Identity Protection è stato configurato.

2.3. Controllare la tua traccia digitale, le violazioni dei dati e le possibili impersonificazioni

Una volta completata la configurazione, Bitdefender Digital Identity Protection esegue una verifica online per scoprire potenziali impersonificazioni, violazioni dei dati e informazioni di identificazione personale sull'open web. Ti consigliamo di verificare ogni singola informazione inclusa nelle schede **TRACCIA DIGITALE**, **VIOLAZIONI DEI DATI** e **CONTROLLO D'IMPERSONIFICAZIONE**.

- Verificare la tua traccia digitale (pagina 10)
- Verificare le violazioni dei dati (pagina 11)
- Verificare le impersonificazioni possibili (pagina 12)

2.4. Migliora il tuo controllo

Usiamo i dati che ci fornisci per monitorare il web superficiale e il Dark web per rilevare qualsiasi attività che possa influenzare la tua privacy o la reputazione del tuo brand personale.

Se vuoi aggiungere un altro indirizzo e-mail o numero di telefono, clicca su ⊕, poi clicca su **AGGIUNGI INDIRIZZO E-MAIL ADDRESS** o **AGGIUNGI NUMERO DI TELEFONO**, e segui le istruzioni.

3. DASHBOARD

La dashboard riunisce le informazioni incluse nelle sezioni **TRACCIA DIGITALE**, **VIOLAZIONI DEI DATI** e **CONTROLLO D'IMPERSONIFICAZIONE**.

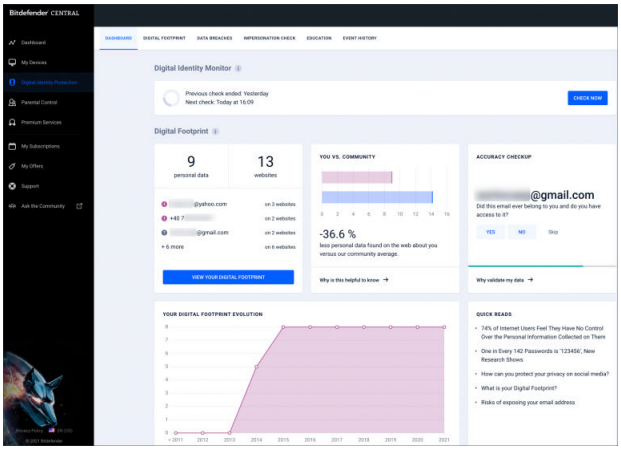
Include le seguenti:

- I tuoi dati esposti e le loro fonti web
- L'ammontare medio di dati esposti per l'intera community
- L'evoluzione della tua traccia digitale
- Contenuti relativi alla privacy
- Violazioni di dati
- Il numero medio di violazioni dei dati nella community

3.1. Monitoraggio identità digitale

Utilizzando solo informazioni accurate, il sistema di Bitdefender cerca nuovi dati personali esposti sull'Open Web e il Dark Web, ed esamina tutte le principali piattaforme dei social media per cercare qualsiasi segno di un tentativo di impersonificazione.

Clicca su **CONTROLLA ORA** per eseguire una scansione online.



4. TRACCIA DIGITALE

Le tue informazioni di identificazione personale e le loro fonti compaiono qui. Sta a te valutare se avere tali informazioni a livello pubblico sul web rappresenti o no una minaccia.

Il nostro monitoraggio guidato dall'IA fa molto affidamento sui dati corretti per rilevare nuove minacce, perciò indicaci se le informazioni sono corrette o poco precise.

Una volta confermato che una parte delle informazioni sono tue, le aggiungiamo al nostro sistema di monitoraggio, migliorando le probabilità di scoprirne altre in futuro.

4.1. Verificare la tua traccia digitale

Per rivedere la tua traccia digitale:

1. Vai alla scheda **TRACCIA DIGITALE**.
2. Le informazioni non ancora verificate compariranno con la dicitura **Verifica** sul lato destro. Clicca su **Verifica** e seleziona Sì o No, a seconda dei casi.

> **Nota**
> Ogni parte di informazione confermata viene aggiunta al nostro algoritmo di monitoraggio, migliorando i risultati mostrati dai nostri servizi. Le informazioni scartate non saranno più visualizzate. Ma, resteranno comunque disponibili sul web.

5. VIOLAZIONI DEI DATI

Le violazioni si verificano quando gli hacker riescono a bypassare le misure di sicurezza di una società e ottengono le tue informazioni personali per venderle sul dark web. In genere, i criminali informatici puntano a dati d'accesso, informazioni di identificazione personale (PII), cartelle cliniche e dati bancari.

Qualsiasi organizzazione o servizio può cadere vittima di una violazione dei dati, ma quelli con un'ampia base di utenti sono bersagli sicuramente più interessanti. Le violazioni incluse normalmente sono nomi, indirizzi e-mail, nomi utente, password, indirizzi postali, numeri di telefono, codici fiscali e dati delle carte di credito (numero, data di scadenza, codice CVV).

5.1. Verificare le violazioni dei dati

Per verificare le tue violazioni dei dati:

1. Vai alla scheda **VIOLAZIONI DEI DATI**.
2. Sotto alcune voci, troverai un elenco di azioni necessarie per proteggere il tuo account. Dopo aver eseguito un'azione, clicca sulla casella accanto a essa per confermarla.
   Se non hai la certezza su come eseguire un'attività, puoi sempre cliccare sul link incluso nella descrizione dell'attività e arriverai a una pagina dove troverai tutti i passaggi necessari.
   Non tutte le violazioni possono essere affrontate in questo modo. Alcune, come **Raccolta #1** non includeranno passaggi. Invece, arriverai ad alcuni articoli disponibili online, dove trovera maggiori aiuto.

> **Nota**
> Bitdefender non memorizza o elabora informazioni di identificazione personale. Vengono mantenuti solo i riferimenti a potenziali violazioni dei dati, senza includere i dati sensibili.

6. CONTROLLO IMPERSONIFICAZIONE

I criminali noti come "impersonificatori" usano l'arte dell'impersonificazione in molti modi, vestendo i panni di un individuo fidato per ingannare le proprie vittime e ottenere accesso a dati sensibili. La pratica del "pretesto" viene definita come presentare sé stessi come qualcun altro per ingannare un destinatario nel fornire dati sensibili come password, numeri di carta di credito o altre informazioni sensibili.

Bitdefender Digital Identity Protection monitora 25 piattaforme social e ti avvisa subito se trovasse un profilo che potrebbe essere un tentativo di impersonificazione.

6.1. Verificare le impersonificazioni possibili

La scheda **CONTROLLO D'IMPERSONIFICAZIONE** è dove saranno mostrati tutti i possibili tentativi. Per ogni rilevamento, puoi scegliere una delle tre possibilità:

- È un tentativo di impersonificazione
- È il tuo profilo personale
- È un profilo differente

In base alla scelta, Bitdefender Digital Identity Protection suggerirà determinati passaggi suggeriti per affrontare il problema. Ogni volta che completi un passaggio, puoi marcarlo come **Fatto**.

7. ISTRUZIONE

La scheda Istruzione funziona come una knowledge base in cui l'utente può trovare più informazioni su come proteggere la sua identità digitale.

Gli articoli indicati qui possono essere ordinati in base a diverse categorie:

- Violazioni
- Esposizioni
- Controllo della rappresentazione

Per accedere alla versione completa di un articolo, clicca sul link **Leggi altro** corrispondente.

8. CRONOLOGIA EVENTO

La sezione Cronologia degli eventi è il mezzo tramite cui comunichiamo costantemente con i nostri utenti. Rappresenta un elenco ordinato cronologicamente di eventi relativi alla protezione della tua traccia digitale.

Oltre alle minacce appena rilevate (nel caso esistessero), puoi tornare a questa pagina per suggerimenti preziosi su come comportarti correttamente online per aumentare le tue probabilità di non incappare in problemi della privacy.

Nella sezione Cronologia degli eventi, puoi trovare le seguenti informazioni:

- Azioni eseguite
- Aggiornamenti del servizio
- Violazioni dei dati

9. DOMANDE FREQUENTI

Perché oggigiorno la privacy online è così importante?

Privacy online significa proteggere i tuoi dati privati e finanziari dai criminali informatici. Tali informazioni di identificazione personale sono molto preziose su Internet e una volta che questi dettagli vengono sottratti, i tuoi soldi non sono più al sicuro. Ti servirà un servizio affidabile per un monitoraggio e una protezione dell'identità costanti per assicurarsi che i tuoi dati privati restino sempre tali.

Qual è la mia traccia digitale?

La tua traccia digitale è la tua intera attività online. Ogni accesso nei tuoi account social, ogni transazione bancaria, tutto ciò che acquisti online possono essere esposti alle violazioni dei dati. Devi essere sempre consapevole del modo in cui i tuoi dati privati e finanziari vengono archiviati e gestiti, e intraprendi i passaggi necessari per proteggerli.

Cosa sono le violazioni dei dati e come influenzano i miei account personali?

Le violazioni dei dati sono incidenti di sicurezza quando i dati privati vengono fatti trapelare in ambienti non sicuri. Questi possono essere sfruttati dai criminali informatici in tutto il mondo per guadagnare accesso alla tua identità online. Le violazioni dei dati possono influenzare il tuo punteggio di credito, l'assicurazione medica, i fondi per il college o persino il tuo fondo pensione.

In che modo Bitdefender Digital Identity Protection può aiutarmi con la mia privacy online?

Bitdefender Digital Identity Protection monitora costantemente i tuoi dati personali, avvisandoti in tempo reale in caso di una violazione dei dati. In questo modo, puoi modificare le tue password e proteggere i tuoi account per prevenire qualsiasi perdita finanziare o impersonificazioni dei social media.

Dove cerca i dati Bitdefender Digital Identity Protection?

Bitdefender Digital Identity Protection cerca i dati sul web superficiale (reti dei social media, post, blog, forum, broker di dati, pubblicazioni, database offline), ma anche sui marketplace del dark web, dove i criminali informatici scambiano le informazioni raccolte dalle violazioni dei dati.

In che modo Bitdefender Digital Identity Protection si differenzia dagli altri servizi (gratuiti)?

Bitdefender Digital Identity Protection ha capacità impareggiabili di monitorare considerevoli volumi e dati di maggiore qualità dal dark web. Le informazioni dal dark web sono curate e deduplicate in modo da poter ridurre gli avvisi di falsi positivi.

Come posso usare il servizio? Devo scaricare qualcosa?

Non devi scaricare nulla, in quanto Bitdefender Digital Identity Protection è un servizio online. Guadagni accesso a una dashboard web dove potrai monitorare tutti gli account personali in tempo reale.

Come posso ricevere gli avvisi per le future violazioni dei dati?

Per ricevere gli avvisi per le future violazioni dei dati puoi semplicemente registrarti per gli avvisi e-mail dalla tua dashboard web e inizierai a ricevere avvisi di privacy e rapporti di sicurezza da Bitdefender Digital Identity Protection.

10. OTTENERE AIUTO

10.1. 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.

10.2. 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.

10.2.1. 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/.

10.2.2. 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/

10.2.3. 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/.

10.3. 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 17).

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

10.3.1. 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 univoca che può essere acquistata al dettaglio e utilizzata per attivare un prodotto o servizio specifico. Un codice di attivazione consente l'attivazione di un abbonamento valido per un certo periodo di tempo e numero di dispositivi e può essere utilizzato anche per estendere un abbonamento con la condizione da generare 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.

Rete privata virtuale (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.