

# Laplink PCdefense™ Guida Introduttiva

011106

**laplink**  
connect your world®

## Come contattare Laplink Software



Per sottoporre domande o problemi di carattere tecnico, visitare il sito:

[www.laplink.com/it/support/individual.asp](http://www.laplink.com/it/support/individual.asp)

Per altri tipi di richieste, è possibile contattare Laplink ai seguenti recapiti.

Indirizzo di posta elettronica: [CustomerService@laplink.com](mailto:CustomerService@laplink.com)

**Tel (IT):** +39 02 91 750719

**Fax (USA):** +1 (425) 952-6002

### Laplink Software, Inc.

14335 NE 24th Street, Suite 201, Bellevue, WA, 98007 U.S.A.

### Comunicazioni Relative al Copyright e ai Marchi

© Copyright 2006 Laplink Software, Inc. Tutti i diritti riservati. Laplink, il logo Laplink, Connect Your World e PCdefense sono marchi registrati o marchi di Laplink Software, Inc. negli Stati Uniti e/o in altri paesi. Altri marchi e prodotti sono di proprietà dei rispettivi titolari.

Grazie per avere scelto PCdefense, la migliore difesa per il computer. Di seguito vengono fornite istruzioni per l'installazione del software e indicazioni passo passo per il primo utilizzo di PCdefense.

## Installazione e configurazione

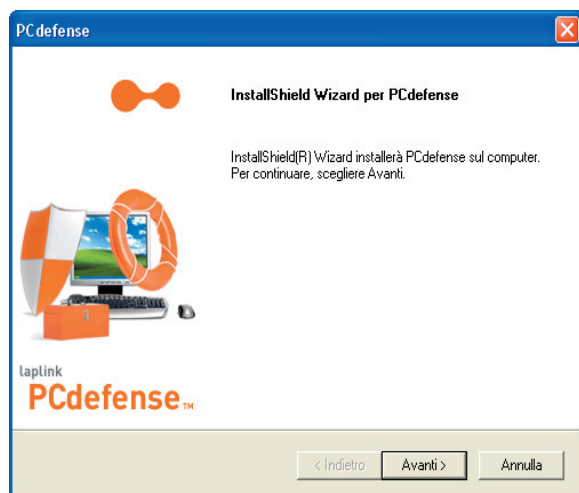
Prima di eseguire l'installazione, assicurarsi che tutti i programmi in esecuzione sul computer siano stati chiusi.

Seguire le istruzioni sotto riportate relative alla modalità di installazione di PCdefense scelta.

**Installazione da CD:** inserire il CD di PCdefense nell'unità CD-ROM/DVD-ROM. Nella schermata di benvenuto di PCdefense, fare clic su **Installare PCdefense**. Se la schermata di benvenuto non viene visualizzata, aprire Esplora risorse e fare doppio clic su PCdefense\_en.exe dal CD-ROM di PCdefense.

**Installazione da un download:** se si esegue il download di PCdefense, fare doppio clic sul file scaricato denominato PCdefense\_en.exe.

**Nota: per installare PCdefense è necessario disporre dei privilegi di amministratore sul computer in uso.**



**Schermata di benvenuto:** fare clic su Avanti per procedere con l'installazione di PCdefense. In qualsiasi schermata è possibile fare clic su Annulla per uscire dall'installazione.

**Contratto di licenza:** fare clic su Sì per accettare il Contratto di licenza di PCdefense oppure su No per uscire dall'installazione del software.

**Informazioni utente:** digitare il proprio nome, il nome della società e il numero di serie. Scegliere Avanti.

**Se il programma è stato installato da CD:** il numero di serie si trova sulla custodia del CD di PCdefense.

**Se PCdefense è stato acquistato online:** in seguito all'acquisto, all'utente viene inviato un messaggio di posta elettronica di conferma. Il numero di serie e il collegamento alla sezione My Downloads di My Support sono specificati all'interno di tale messaggio. Nella sezione My Downloads, è possibile richiedere una copia del software PCdefense, ottenere il proprio numero di serie e altro ancora.

Per accedere all'account My Support, collegarsi al sito:

[www.laplink.com/it/support/individual.asp](http://www.laplink.com/it/support/individual.asp)

e immettere il nome utente e la password.

**Scegliere il percorso di destinazione:** scegliere l'unità e la directory in cui installare PCdefense, oppure accettare il percorso predefinito. Fare clic su Avanti quando si è pronti.

**Avvio della copia dei file:** PCdefense dispone di tutte le informazioni necessarie per eseguire l'installazione. Esaminare le impostazioni correnti e fare clic su Indietro per apportare eventuali modifiche oppure su Avanti per continuare.

PCdefense sarà installato sul PC. Fare clic su **Fine** al termine dell'installazione.

## Introduzione - Registrazione

La prima volta che si apre PCdefense, viene visualizzata una finestra popup che indica che si hanno a disposizione 30 giorni per registrare il programma. Per effettuare subito la registrazione scegliere Sì, altrimenti fare clic su No ed eseguire l'operazione in un secondo tempo.

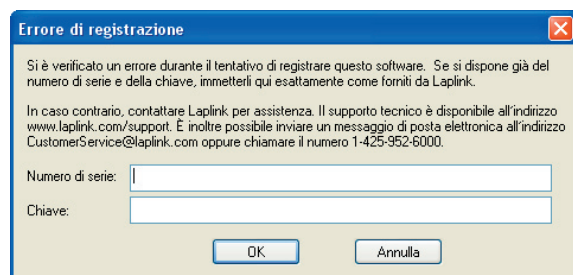
Verrà visualizzata la schermata illustrata sopra. Il numero di serie viene automaticamente inserito nell'apposito campo. Specificare le informazioni come indicato e assicurarsi di fornire un indirizzo di posta elettronica valido. Una volta eseguita la registrazione di PCdefense, questa schermata non sarà più visualizzata.

È possibile scegliere di non visualizzare questa schermata. La schermata verrà visualizzata all'avvio fino a quando non si registra PCdefense. **Per continuare a utilizzare PCdefense, è necessario registrare il software entro 30 giorni dall'installazione.**

**Nota: è necessario registrare PCdefense prima di creare immagini di Disaster Recovery.**

### Se non è possibile eseguire la registrazione...

Se per qualche motivo non è possibile eseguire la registrazione (numero di serie non valido, immissione non corretta del numero di serie, errore di connessione a Internet, ecc.), verrà visualizzata la seguente schermata.



Se viene visualizzata questa schermata, è necessario contattare il supporto tecnico di Laplink tramite posta elettronica o telefono.

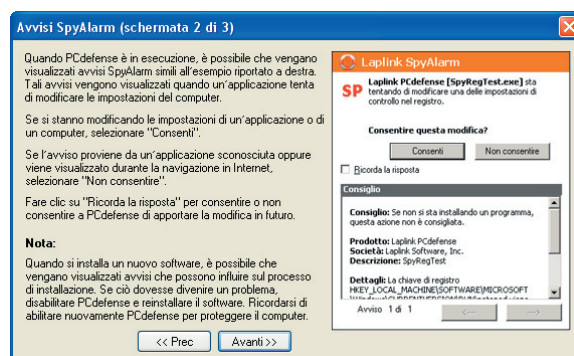
- **Posta elettronica - CustomerService@laplink.com**
- **Telefono - + 39 02 91 750719**

Gli addetti all'assistenza clienti di Laplink convalideranno l'acquisto del prodotto e forniranno al cliente i relativi numero di serie e chiave per consentirgli di registrare correttamente PCdefense.

### Informazioni introduttive

Successivamente alla finestra per la registrazione, verranno visualizzate tre pagine popup, che sono essenziali per comprendere il funzionamento di PCdefense e scoprire come utilizzarlo.

La prima pagina fornisce un'introduzione a PCdefense e ne presenta le funzionalità principali. Fare clic su **Avanti** quando si è pronti.

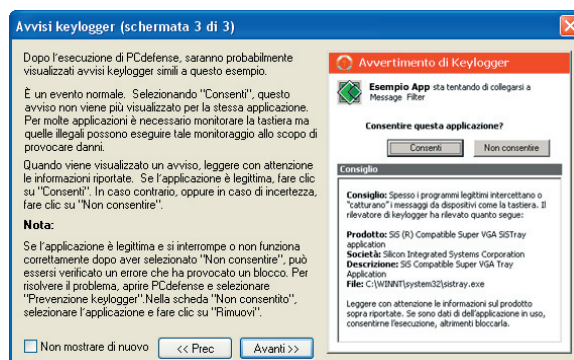


Nella schermata seguente, sopra illustrata, viene descritto il funzionamento del monitoraggio di SpyAlarm. Gli avvisi di SpyAlarm vengono visualizzati quando un'applicazione tenta di modificare alcune impostazioni del computer. Se tali avvisi vengono visualizzati durante la modifica manuale delle impostazioni del PC, è probabile che il computer non sia esposto a pericoli, ed è possibile selezionare il pulsante **Consenti**. Se invece l'avviso viene visualizzato durante la navigazione in Internet, quando non si stanno apportando modifiche al programma, selezionare il pulsante **Non consentire**.

Fare clic sulla casella di controllo **Ricorda la risposta** per consentire a PCdefense di ricordare la scelta effettuata e gestire il programma sempre allo stesso modo.

Fare clic su **Avanti** quando si è pronti.

Nella schermata successiva vengono forniti suggerimenti su come interpretare gli avvisi keylogger.



Gli avvisi keylogger vengono visualizzati quando determinati programmi tentano di collegarsi alla tastiera. Durante l'apertura e l'installazione delle applicazioni, questo comportamento è normale, pertanto è possibile selezionare il pulsante **Consenti**.

Se invece gli avvisi keylogger vengono visualizzati durante la navigazione in Internet, oppure quando non

si eseguono operazioni di installazione o apertura dei programmi, fare clic sul pulsante Non consentire.

Per informazioni dettagliate sul monitoraggio di SpyAlarm, la prevenzione keylogger e tutte le potenti funzionalità offerte da PCdefense, consultare la Guida per l'utente di PCdefense.

### Primo utilizzo di PCdefense

A meno che PCdefense non venga installato su un computer completamente nuovo, è consigliabile eseguire immediatamente una scansione per pulire il computer e modificarne le impostazioni al fine di evitare nuove infezioni.

PCdefense è impostato in modo tale che l'utente debba semplicemente accettare le impostazioni predefinite visualizzate in ogni schermata per eseguire correttamente la pulizia e la manutenzione del PC. Per istruzioni dettagliate su come definire le scansioni e gestire la creazione dell'immagine di Disaster Recovery, consultare la Guida per l'utente di PCdefense.

Per pulire il PC con PCdefense, seguire la procedura illustrata nella presente Guida introduttiva, accettando tutte le impostazioni predefinite.

### Passaggio uno: eseguire Spyware Scan

Sebbene esistano numerose definizioni, per "spyware" generalmente si intende qualsiasi programma software che sfrutti la connessione a Internet di un utente senza che questi ne sia al corrente o abbia dato il suo permesso esplicito. Spyware Scan consente di eseguire la scansione del PC alla ricerca di spyware installati nel computer. Inoltre permette di decidere quale azione eseguire nel caso venga rilevata un'intrusione.

#### Per eseguire Spyware Scan:

In PCdefense, scegliere Spyware Scan tra le opzioni di difesa.

1. Fare clic sul pulsante Esegui Spyware Scan.
2. All'apertura della pagina di Spyware Scan, fare clic sul pulsante Avvia per avviare la procedura di scansione del PC.
3. Al termine della scansione, verrà visualizzato un elenco di file considerati spyware, che mettono a rischio la sicurezza del PC. Tutti i file verranno selezionati per impostazione predefinita. Visualizzare l'elenco dei file e deselezionare quelli che PCdefense deve ignorare. Al termine dell'operazione, fare clic su Rimuovi per eliminare tutti i file contrassegnati.

Gli spyware individuati verranno messi in quarantena nel PC in uso. Se lo si desidera, è possibile scegliere di

eliminarli in modo permanente più avanti.

**Nota: il processo di scansione alla ricerca di spyware può avere una durata che va da pochi minuti a un'ora o più, in base alle opzioni di scansione scelte e alle dimensioni e la velocità del computer.**

### Passaggio due: eseguire la scansione antivirus

La possibilità di navigare in Internet per ottenere informazioni, strumenti software, nozioni finanziarie e molto altro ancora ha trasformato il PC in una preziosa fonte di informazioni, divertimento e comunicazione. Tuttavia, lo svolgimento di queste attività presenta delle insidie in quanto, a insaputa dell'utente, sul computer possono venire installati malware e virus. Lo strumento di ricerca Laplink Online Virus Scan è un prodotto antivirus completo che fornisce tutti gli elementi necessari alla ricerca e alla conseguente eliminazione dei virus: esegue la scansione della memoria del sistema, di tutti i file, cartelle e settori di avvio delle unità e consente di eliminare automaticamente i file infetti.

Nota: è anche possibile scegliere di definire ulteriori opzioni e impostazioni di scansione antivirus. Per visualizzare le opzioni disponibili, selezionare i collegamenti presenti nella pagina di scansione. Per maggiori informazioni sulle opzioni di scansione disponibili è possibile consultare la Guida per l'utente di PCdefense.

#### Per eseguire la scansione antivirus:

In PCdefense, scegliere Scansione antivirus tra le opzioni di difesa.

1. Fare clic sul pulsante **Esegui scansione antivirus**.
2. All'apertura della relativa pagina, avviare la scansione del PC facendo clic sul pulsante Fare clic qui per avviare una nuova scansione.

Con la scansione antivirus verranno rilevati e immediatamente eliminati eventuali virus presenti nel PC.

Nota: per utilizzare la scansione antivirus è necessario installare un controllo ActiveX.

**Nota: il processo di scansione alla ricerca di virus può avere una durata che va da pochi minuti a un'ora o più, in base alle opzioni di scansione scelte e alle dimensioni e la velocità del computer.**

### Passaggio tre: eseguire una scansione per la ricerca di rootkit

I rootkit rappresentano la minaccia più seria di ultima

generazione per i PC. Possono eseguire le stesse funzioni dei keylogger, virus o altri malware o spyware, ma non essere rilevati da programmi antispyware e antivirus, in quanto si nascondono bene nei PC.

### Definizione di rootkit

Per "rootkit" si intende un insieme di strumenti (programmi) che permette di accedere con autorizzazioni di amministratore a un computer o a una rete di computer. In genere, un hacker installa un rootkit in un computer dopo averne ottenuto l'accesso a livello utente, mediante lo sfruttamento di una vulnerabilità nota o il crack di una password. Una volta installato, il rootkit permette all'intruso di non essere rilevato e di ottenere l'accesso con privilegi di amministratore al computer ed eventualmente ad altre macchine connesse in rete.

Un rootkit può essere composto da spyware e altri programmi che eseguono il monitoraggio del traffico e delle sequenze di tasti utilizzati. Talvolta i rootkit creano una "porta di servizio" nel sistema a uso dell'hacker, modificano i file di registro, attaccano altri computer connessi in rete e alterano gli strumenti di sistema esistenti per non essere rilevati. La diffusione dei rootkit cresce sempre più e le fonti da cui provengono sono sempre più sorprendenti. Gli esperti temono che siano molto più diffusi di quanto non si sospetti.

I rootkit non possono essere rilevati in modo convenzionale, ovvero mediante la ricerca negli elenchi dei file o nel Registro di sistema. In genere, i programmi antivirus e antispyware standard non sono in grado di rilevare né tantomeno eliminare i rootkit.

### Utilizzo della scansione per la ricerca di rootkit di PCdefense

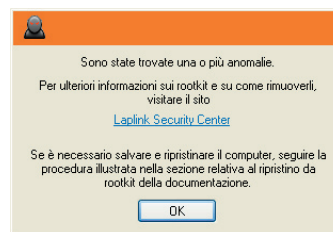
Se si rileva un rootkit in un sistema, si consiglia di rimuoverlo in quanto può agire come spyware o keylogger, e può acquisire e trasmettere i dati personali dell'utente all'origine.

Per informazioni sulla rimozione dei rootkit dal PC, consultare la Guida per l'utente di PCdefense.

### Eseguire la scansione per la ricerca di rootkit

In PCdefense, scegliere Scansione per la ricerca di rootkit tra le opzioni di difesa.

- Fare clic sul pulsante Esegui scansione per la ricerca di rootkit sul PC per rilevare la presenza di eventuali rootkit:



### Se si rileva un rootkit...

Se nel computer in uso viene rilevata un'anomalia, che può essere un rootkit, sarà visualizzata la schermata qui sopra illustrata. Fare clic sul collegamento presente in questa finestra per collegarsi al **Laplink Security Center**, in cui è possibile reperire informazioni su anomalie comuni e suggerimenti sulle operazioni da eseguire.

La scansione per la ricerca di rootkit di PCdefense consente di rilevare i rootkit utilizzando metodi diversi. Tra i metodi proprietari sono inclusi:

- Rilevamento di processi nascosti
- Hook di moduli online nascosti
- Rilevamento di driver del kernel nascosti
- Hook di driver del kernel nascosti

### Passaggio quattro: creare un'immagine di Disaster Recovery

Disaster Recovery (DR) di PCdefense permette di creare un'immagine sicura di backup del PC in uso, fornisce assistenza nella fase di creazione del backup su altre unità o supporti e consente di ripristinare la copia di backup nel sistema.

### Prepararsi alle emergenze

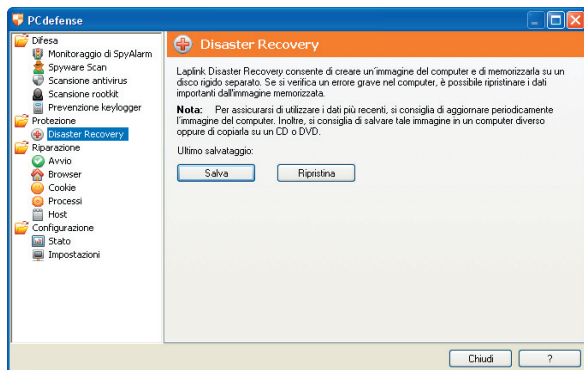
È possibile che l'utilizzo di strumenti come PCdefense garantisca la protezione del computer e impedisca l'insorgere di problemi. Ma cosa fare se qualcosa si rompe o viene rubato? Cosa fare se il computer smette di funzionare? Si dispone di un backup completo, e non solo di alcuni file, di tutto ciò che si trova nel computer, di tutti i programmi utilizzati, di tutti i messaggi di posta elettronica, di tutti i file e le impostazioni?

Indipendentemente dal modo in cui avviene il problema (a causa di un virus, di un hacker o di una tazza di caffè rovesciata sul PC), i computer possono subire danni e, di conseguenza, si possono perdere dati importanti.

PCdefense include Disaster Recovery, uno strumento che permette di creare un'immagine di backup completo del sistema. Ciò significa che, indipendentemente da ciò che accade, si può sempre disporre di una copia di backup sicura dei dati presenti nel computer.

Disaster Recovery (DR) è uno strumento che consente di far fronte a eventuali emergenze che compromettono l'utilizzo dei dati presenti nel computer, quali un blocco del sistema o lo smarrimento del PC; non è uno strumento per il backup quotidiano. PCdefense crea un'immagine di tutti i dati contenuti nel PC al fine di ripristinarli nel caso in cui si verifichi un'emergenza. Quanto più frequentemente si aggiorna l'immagine, tanto più improbabile risulta la perdita dei dati.

## Creazione di un'immagine di Disaster Recovery



**Nota:** per utilizzare Disaster Recovery, è necessario disporre dei privilegi di amministratore sul computer in uso.

### 1. Definire l'immagine di DR

In PCdefense, nell'opzione Protezione, fare clic su Disaster Recovery. Fare clic su **Salva** per avviare l'operazione.

Disaster Recovery ripristina ogni file e impostazione di registro non esistente durante il ripristino. Non viene sovrascritto nulla. Le impostazioni hardware e le cartelle temporanee non vengono ripristinate, il che significa che, se è necessario eseguire il ripristino in un nuovo PC, l'operazione può essere comunque effettuata. Queste sono le impostazioni e le opzioni più comunemente incluse in un'immagine.

Nella pagina principale della procedura guidata creazione immagine, è possibile accettare le impostazioni predefinite facendo clic sul pulsante **Avanti**.

**IMPORTANTE! Salvare l'immagine in una posizione diversa!**

**Se il PC ha subito un danno catastrofico, è possibile perdere in maniera permanente tutti i dati archiviati nelle unità locali, incluse le immagini di Disaster Recovery salvate in queste unità. Si consiglia di salvare le immagini in un'unità di rete, su un CD o in un altro PC. Assicurarsi di archiviare almeno una copia delle immagini di Disaster Recovery in un luogo sicuro al di**

**fuori del PC.**

### 2. Creare componenti per l'immagine

Nella schermata successiva, fare clic su **Avanti** per avviare la creazione dei componenti necessari a generare l'immagine di Disaster Recovery.

#### Eseguire il mapping degli utenti

Il primo componente è Esegui mapping utenti. In questa schermata è possibile decidere se includere o escludere gli utenti nel PC in uso.

Per accettare tutti gli utenti (impostazione di sistema predefinita) e proseguire con la creazione dell'immagine di Disaster Recovery, fare clic su **Chiudi**.

**Per includere o escludere un utente:** dall'immagine di DR, selezionare l'utente e fare clic sul pulsante Escludi o Includi. Gli utenti normali sono visualizzati per impostazione predefinita.

#### Eseguire il mapping delle unità

Disaster Recovery consente di scegliere quali unità includere o escludere nell'immagine di Disaster Recovery.

Per includere o escludere una delle unità elencate, fare clic sull'unità per selezionarla, quindi fare clic sul pulsante Includi o Escludi.

Dopo avere selezionato le unità da includere nell'immagine di Disaster Recovery, fare clic su **Chiudi**.

Nella schermata successiva verrà visualizzato lo stato di avanzamento della creazione dell'immagine.

### 3. Assegnare un nome all'immagine di DR

Nella schermata successiva è necessario specificare un nome per l'immagine di DR.

L'immagine di Disaster Recovery rappresenta un backup dei file e dei dati presenti nell'intero sistema, che possono essere di grandi dimensioni. **Agli utenti si consiglia di:**

**Scrivere l'immagine di DR su un'unità di rete o una periferica esterna (Disaster Recovery consente la scrittura su CD/DVD) in modo tale che, in caso di blocco del sistema, il backup si trovi in un luogo sicuro.**

Dopo avere scelto un'unità in un luogo sicuro e dotata di spazio sufficiente, fare clic su **Avanti**.

### 4. Opzioni di archiviazione dei dati

PCdefense e Disaster Recovery consentono di suddividere il backup in più parti. Questa funzione è utilizzata principalmente durante la scrittura su CD. Per impostazione predefinita, l'immagine viene suddivisa in parti da 600 megabyte, ovvero la quantità di dati che è possibile archiviare sui CD scrivibili standard.

Scegliere la dimensione del file che meglio soddisfa le esigenze dell'immagine di Disaster Recovery, quindi fare clic su Avanti.

### 5. Creare l'immagine di Disaster Recovery

A questo punto, PCdefense dispone di tutte le informazioni necessarie per la creazione dell'immagine di DR. Per avviare il processo di creazione dell'immagine, fare clic su Avanti.

Il processo di creazione dell'immagine di Disaster Recovery può durare pochi minuti o più ore, in base alla quantità di dati da generare e altri fattori.

Congratulazioni! È in corso la creazione dell'immagine di Disaster Recovery. Al termine dell'operazione, **assicurarsi di archiviare una copia dell'immagine in un altro luogo.**

### Passaggio cinque: assicurarsi che le funzioni di monitoraggio di SpyAlarm e di prevenzione keylogger siano abilitate

Entrambe le funzioni di **Monitoraggio di SpyAlarm** e di **Prevenzione Keylogger** sono abilitate per impostazione predefinita, ma è importante comprenderne il funzionamento.

Il **Monitoraggio di SpyAlarm** impedisce che le applicazioni vengano installate sul sistema senza il consenso dell'utente. Alcuni spyware vengono installati senza che l'utente se ne accorga. Quando un'applicazione tenta di scrivere su aree delicate del sistema Windows, il monitoraggio di SpyAlarm visualizza un messaggio popup, grazie al quale è possibile controllare se un'applicazione è autorizzata ad apportare modifiche al sistema.

La funzione **Prevenzione Keylogger** impedisce ai keylogger installati nel PC di raccogliere i dati dell'utente. Un keylogger è un programma o una periferica hardware progettata per registrare le sequenze di tasti utilizzati. Può trattarsi di una periferica hardware (installata sulla tastiera) o di un programma software che esegue la registrazione dei tasti selezionati. La funzione Prevenzione keylogger impedisce ai keylogger di vedere quali tasti vengono selezionati.

**Nota: quando un keylogger viene rilevato da PCdefense e si seleziona il pulsante Non consentire nell'avviso popup, è necessario riavviare il computer per disabilitare il keylogger in modo permanente e impedirgli di agire nel PC in uso.**

Per accedere al controllo di **Monitoraggio di SpyAlarm**, nella cartella Configurazione scegliere l'opzione Impostazioni. Per selezionare o deselezionare questa

opzione, fare clic sul pulsante Abilita monitoraggio di SpyAlarm.

Per accedere al controllo **Prevenzione Keylogger**, nella scheda Difesa delle opzioni di PCdefense, fare clic su **Prevenzione** keylogger. Per selezionare o deselezionare questa opzione, fare clic sul pulsante Attiva/Disattiva.

**Congratulazioni!** Il computer è ora privo di virus e spyware, e sono state impostate delle difese per evitare che questi attacchino nuovamente il sistema in futuro. Un'immagine nuova di Disaster Recovery è stata creata e salvata in una posizione differente.

## Altre funzionalità di PCdefense

### Programmi di avvio

I programmi elencati in questa schermata di PCdefense sono stati aggiunti al gruppo di avvio dall'utente o in fase di installazione di un programma. Tali programmi vengono eseguiti in seguito all'esecuzione di Windows. Sebbene disabilitare programmi sia generalmente un'operazione sicura, è importante comprendere il funzionamento di un programma prima di disabilitarlo, in quanto in seguito a tale operazione il sistema può risultare instabile. In caso di dubbi sull'esecuzione di questa operazione, contattare il fornitore del software.

#### Utente corrente e Macchina

- I programmi possono essere posizionati in gruppi di avvio differenti.
- I programmi inclusi nelle schede Macchina sono impostati per essere eseguiti all'avvio della macchina, indipendentemente da chi si connette al PC.
- I programmi inclusi nelle schede Utente corrente vengono avviati quando l'utente corrente si connette al PC

I programmi possono essere impostati per l'avvio in entrambi i gruppi.

**Nota: assicurarsi di comprendere il funzionamento del programma di avvio prima di disabilitarlo, in quanto tale operazione può causare problemi al PC.**

### Browser

Il browser installato nel computer che si acquista presenta alcune impostazioni predefinite. Certi tipi di spyware e malware possono modificare tali impostazioni, reindirizzando l'utente al loro motore di ricerca, chiedendogli se desidera installare il loro software oppure impostando il loro sito come home page. La funzione di ripristino del browser di PCdefense permette di ripristinare le impostazioni predefinite del

browser con la semplice selezione di un pulsante.

Tutte le impostazioni predefinite del sistema sono elencate nella finestra di ripristino del browser di PCDefense. Se per qualche motivo viene modificata un'impostazione predefinita, incluse le modifiche manuali apportate da un utente, tale impostazione verrà evidenziata in blu nella colonna Corrente.

### Cookie

I cookie sono file che vengono collocati nel PC quando si accede a un sito Web in modo da permettere al sito di ricordare le informazioni relative all'utente anche successivamente. In genere i cookie non sono dannosi, ma è possibile che alcuni siti li utilizzino a insaputa degli utenti. Ciò può rivelarsi pericoloso per i dati contenuti nel computer o per il sistema stesso. PCdefense consente di eliminare i cookie dal sistema in modo rapido e semplice.

#### Opzioni dei cookie

**Rimuovi-** Selezionare un cookie, quindi fare clic su Rimuovi per eliminarlo dal PC.

**Rimuovi tutto-** Questa opzione permette di rimuovere tutti i cookie dal PC.

**Visualizza-** Questa opzione consente di visualizzare il contenuto di un cookie in un file di testo.

**Dettagli-** Questa opzione permette di visualizzare i dettagli relativi al cookie selezionato, che includono: l'URL di origine, il nome del cookie memorizzato localmente, informazioni su date, l'ultimo accesso al cookie e la data di scadenza del cookie.

**Proprietà-** (in Dettagli)- Questa opzione consente l'apertura della finestra di dialogo Proprietà di Windows, in cui è possibile modificare gli attributi, rinominare il file e accedere a tutte le funzionalità disponibili nella finestra di dialogo delle proprietà di Windows.

### Processi

Sebbene quasi tutti i processi in esecuzione nel computer siano normali e sicuri, anche gli spyware e i malware possono essere eseguiti come processi. Per arrestare qualsiasi processo in esecuzione nel sistema, è possibile utilizzare la scheda Processi in PCdefense.

**Termina-** Scegliendo questa opzione, è possibile terminare immediatamente l'esecuzione di un processo nel PC. Ciò può produrre risultati non desiderati, come la perdita di dati e l'instabilità del sistema. Il processo non potrà modificare lo stato o i dati prima di essere terminato.

**Proprietà-** Questa opzione consente l'apertura della finestra di dialogo Proprietà di Windows, in cui è possibile modificare gli attributi, rinominare il file e accedere a tutte le funzionalità disponibili nella finestra di dialogo delle proprietà di Windows.

Nella finestra di dialogo delle proprietà sono visualizzate

anche informazioni sul processo, quali il produttore del software, la versione, informazioni sulla sicurezza e altro ancora. Questi dati possono essere utili per determinare se il processo selezionato è affidabile o sospetto, nel cui caso potrebbe trattarsi di spyware o malware.

**Dettagli-** Selezionando il pulsante Dettagli, è possibile visualizzare i file di libreria a collegamento dinamico (DLL) collegati all'applicazione selezionata. In questo modo è possibile identificare i malware in esecuzione nel sistema.

Talvolta gli spyware o i virus sono collegati a un'applicazione frequentemente utilizzata, come Internet Explorer, sotto forma di file DLL. Nella finestra Dettagli è possibile visualizzare tutti i file DLL collegati a una particolare applicazione. Se sono presenti file DLL non riconoscibili o si sospetta che questi non siano collegati a un'applicazione affidabile, è possibile eseguire una ricerca in Internet per trovare informazioni su tali file e, se necessario, disabilitare o eliminare il processo o il file sospetto.

### File Hosts

Il file Hosts è paragonabile a una rubrica. Quando si digita un indirizzo Web, come www.laplink.com, nella barra degli indirizzi del browser, il file Hosts viene consultato per verificare la presenza dell'indirizzo IP di tale sito. Se tale indirizzo è presente, il computer eseguirà la connessione e il sito verrà aperto. Alcuni spyware/malware possono modificare la tabella HOSTS al fine di reindirizzare un sito Web a un indirizzo differente, rimandando l'utente a un sito spyware/malware a sua insaputa.

### Impostazioni

Nella finestra Impostazioni di PCdefense sono fornite informazioni sui file di registro creati durante l'utilizzo del software. Questi file forniscono informazioni sulle ultime scansioni effettuate, gli avvisi software visualizzati, le azioni eseguite e altri importanti elementi. La finestra Impostazioni consente inoltre di attivare o disattivare alcune funzionalità.

### Impostazioni di PCdefense

Le funzionalità contrassegnate da un segno di spunta verde nella finestra Impostazioni sono attivate.

**File registro-** Contiene un elenco di tutti gli avvisi generati in PCdefense.

**Cronologia avvisi-** Il file Cronologia avvisi contiene una descrizione completa di tutti gli avvisi, incluse la data in cui sono stati generati, le azioni intraprese e la chiave di registro.

**Avvisi salvati-** Il file Avvisi salvati tiene traccia di tutti gli avvisi che si è scelto di "ricordare".