

---

Subject: KeyLogger

Posted by [Trink](#) on Mon, 08 Aug 2011 10:57:45 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

Temo che sulla mia macchina sia stato installato un KeyLogger, Ubuntu 11.04  
Come posso fare per escludere con certezza tale evenienza?

--

---

---

Subject: Re: KeyLogger

Posted by [Fandango](#) on Mon, 08 Aug 2011 11:44:48 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

On Mon, 08 Aug 2011 10:57:45 +0000, Trink wrote:

> Temo che sulla mia macchina sia stato installato un KeyLogger, Ubuntu 11.04  
> Come posso fare per escludere con certezza tale evenienza?

chi ha messo il keylogger ed il perchÃ

---

---

Subject: Re: KeyLogger

Posted by [Fandango](#) on Mon, 08 Aug 2011 11:45:12 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

On Mon, 08 Aug 2011 10:57:45 +0000, Trink wrote:

> Temo che sulla mia macchina sia stato installato un KeyLogger, Ubuntu 11.04  
> Come posso fare per escludere con certezza tale evenienza?

Se Ã sul tuo computer di casa Ã una questione, se Ã sul tuo computer in ufficio Ã ben altra cosa.

---

---

Subject: Re: KeyLogger

Posted by [Fandango](#) on Mon, 08 Aug 2011 11:47:51 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

On Mon, 08 Aug 2011 10:57:45 +0000, Trink wrote:

> Temo che sulla mia macchina sia stato installato un KeyLogger, Ubuntu 11.04  
> Come posso fare per escludere con certezza tale evenienza?

<http://wiki.ubuntu-it.org/Sicurezza>

---

---

Subject: Re: KeyLogger

Posted by [The\\_ZiPMaN](#) on Mon, 08 Aug 2011 12:38:40 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

On 08/08/2011 12:57 PM, Trink wrote:

> Come posso fare per escludere con certezza tale evenienza?

Dipende... inizierei con il controllare se vi Ã" qualche tua digitazione scritta in chiaro su qualche file. Per verificare questo digiti una sequenza di testo ben precisa (p.es. 98761234asdfgtrewq stando attento a non premere alcunchÃ© d'altro, specie shift, ctrl e alt) e poi cerchi in tutti i files se questa combinazione compare da qualche parte:

```
find / -type f -mtime -1 -print0 | xargs -0 grep -l 98761234asdfgtrewq
```

Se non trova nulla puoi fare un giro di rkhunter e/o chkrootkit opportunamente aggiornati e vedere se scoprono qualcosa.

--

Flavio Visentin

Scientists have finally discovered what's wrong with the female brain:  
On the left side, there is nothing right, and on the right side, there is nothing left.

---

---

Subject: Re: KeyLogger

Posted by [ivanterzo](#) on Mon, 08 Aug 2011 12:40:36 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

Il 08/08/2011 12:57, Trink ha scritto:

> Temo che sulla mia macchina sia stato installato un KeyLogger, Ubuntu 11.04

> Come posso fare per escludere con certezza tale evenienza?

>

scusa se non rispondo esattamente alla domanda, del resto le indicazioni che dai sono realmente poche.

Quello che voglio domandarti e' pero' questo; cosa ti fa supporre che sulla macchina sia installato un keylogger? Ovvero, che indizi hai?

Ultimamente hai forse installato qualche programma scaricato da qualche sito non sicuro? E come lo hai installato? Come root o come semplice utente?

Che sintomi presenta la tua macchina? Se crei un account di test avverti gli stessi sintomi o sospetti?

--

Pandozy vede tutto

O',=,'O  
(0 0)  
ooO--( )--Ooo

---

---

Subject: Re: KeyLogger

Posted by [Trink](#) on Mon, 08 Aug 2011 15:30:06 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

ivanterzo ha scritto:

>Il 08/08/2011 12:57, Trink ha scritto:

>> Temo che sulla mia macchina sia stato installato un KeyLogger, Ubuntu 11.04

>> Come posso fare per escludere con certezza tale evenienza?

>>

>

>scusa se non rispondo esattamente alla domanda, del resto le indicazioni

>che dai sono realmente poche.

>

>Quello che voglio domandarti e' pero' questo; cosa ti fa supporre che

>sulla macchina sia installato un keylogger? Ovvero, che indizi hai?

>

>Ultimamente hai forse installato qualche programma scaricato da qualche

>sito non sicuro? E come lo hai installato? Come root o come semplice utente?

>

>Che sintomi presenta la tua macchina? Se crei un account di test avverti

>gli stessi sintomi o sospetti?

Sintomi e sospetti ci sono. Non posso specificare ma ci sono.

O si tratta di Keylogger o di sniffing dalla rete.

Nel secondo caso cosa fare? Apro un nuovo post o continuiamo su questo (per lo sniff)?

--

---

---

Subject: Re: KeyLogger

Posted by [Trink](#) on Mon, 08 Aug 2011 15:46:31 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

The\_ZiPMaN ha scritto:

>On 08/08/2011 12:57 PM, Trink wrote:

>> Come posso fare per escludere con certezza tale evenienza?

>

>Dipende... inizierei con il controllare se vi è qualche tua digitazione

>scritta in chiaro su qualche file. Per verificare questo digiti una  
>sequenza di testo ben precisa (p.es. 98761234asdfgtrewq stando attento a  
>non premere alcunché d'altro, specie shift, ctrl e alt) e poi cerchi in  
>tutti i files se questa combinazione compare da qualche parte:

```
>  
>find / -type f -mtime -1 -print0 | xargs -0 grep -l 98761234asdfgtrewq
```

Ci sono parecchi file a cui viene negato l'accesso anche se uso sudo.

>Se non trova nulla puoi fare un giro di rkhunter e/o chkrootkit  
>opportunamente aggiornati e vedere se scoprono qualcosa.

Ho provato rkhunter e su /usr/bin/mail mi ha dato un [ Warning ],  
/usr/bin/bsd-mailx [ Warning ]

Performing filesystem checks

```
  Checking /dev for suspicious file types          [ Warning ]  
  Checking for hidden files and directories        [ Warning ]
```

System checks summary

=====

File properties checks...

```
  Files checked: 132  
  Suspect files: 2
```

Rootkit checks...

```
  Rootkits checked : 242  
  Possible rootkits: 0
```

Applications checks...

```
  All checks skipped
```

The system checks took: 2 minutes and 51 seconds

All results have been written to the log file (/var/log/rkhunter.log)

One or more warnings have been found while checking the system.  
Please check the log file (/var/log/rkhunter.log)

chkrootkit non trova nulla.

Cosa fare per i Warning? Per eventuale sniff quale procedura seguire per  
verificare approfonditamente?

--

---

Subject: Re: KeyLogger  
Posted by [Roberto](#) on Mon, 08 Aug 2011 15:52:10 GMT  
[View Forum Message](#) <> [Reply to Message](#)

---

Trink ha scritto:  
-cut-

> Sintomi e sospetti ci sono. Non posso specificare ma ci sono.

Domestico o aziendale?

Nel primo caso, reinstalla da pulito, se non ti fidi del tuo pc.  
Nel secondo caso, posta su it.lavoro.\* per cercarti un altro posto.

--

|Save our planet!  
Ciao |Save wildlife!  
roberto |For your E-MAIL use ONLY recycled Bytes !!  
|roberto poggi rpoggi@softhome.net

---

---

Subject: Re: KeyLogger  
Posted by [Enrico 'Henryx' Bianc](#) on Mon, 08 Aug 2011 22:48:49 GMT  
[View Forum Message](#) <> [Reply to Message](#)

---

Trink wrote:

> Ci sono parecchi file a cui viene negato l'accesso anche se uso sudo.

Se sono sotto /proc /sys e /run e` normale

Enrico

---