Subject: Controllare a posteriori gli aggiornamenti
Posted by Trink on Thu, 28 Jul 2011 05:38:59 GMT
View Forum Message <> Reply to Message

Visto che gli hackerognoli se ne inventano una al minuto volevo sapere come controllare a posteriori che gli aggiornamenti installati sono effettivamente originali e certificati ubuntu. Di recente, come da mio post precedente, non ho avuto una bella esperienza. Grazie 1000!

--

Subject: Re: Controllare a posteriori gli aggiornamenti
Posted by Roberto on Thu, 28 Jul 2011 07:46:38 GMT
View Forum Message <> Reply to Message

Trink ha scritto:
> Visto che gli hackerognoli se ne inventano una al minuto volevo sapere come
> controllare a posteriori che gli aggiornamenti installati sono effettivamente

A posteriori non puoi, a meno di non avere una copia della macchina precedente all'aggiornamento su cui rifare l'aggiornamento *sicuro* da confrontare con l'altra.

> originali e certificati ubuntu. Di recente, come da mio post precedente, non
> ho avuto una bella esperienza. Grazie 1000!

Hai avuto solo fretta e un pizzico di superficialitÃ .

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

Subject: Re: Controllare a posteriori gli aggiornamenti
Posted by Trink on Fri, 29 Jul 2011 10:20:56 GMT
View Forum Message <> Reply to Message

roberto ha scritto:
>Trink ha scritto:
>> Visto che gli hackerognoli se ne inventano una al minuto volevo sapere come
>> controllare a posteriori che gli aggiornamenti installati sono effettivamente
>

>A posteriori non puoi, a meno di non avere una copia della macchina
>precedente all'aggiornamento su cui rifare l'aggiornamento *sicuro*
>da confrontare con l'altra.

Uhmm... pero', ad esempio, non esiste una lista dei pacchetti di aggiornamento
ufficiali e una lista di quanto installato? In effetti non potrebbe esserci un
checksum di quanto installato e come doveva essere?
Si potrebbe implementare uno strumento che confronta queste due liste,
periodicamente, e vedere se tutto e' ok o ci sono differenze.
Vado oltre? (tanto oltre che se guardo dietro vedo il futuro? (autoironia))
Giusto come proposta da niubbo.

>> originali e certificati ubuntu. Di recente, come da mio post precedente,
non
>> ho avuto una bella esperienza. Grazie 1000!
>
>Hai avuto solo fretta e un pizzico di superficialiti¿½.

Distrazione telefonica, ahime'...

--

Subject: Re: Controllare a posteriori gli aggiornamenti
Posted by Roberto on Fri, 29 Jul 2011 10:44:39 GMT
View Forum Message <> Reply to Message

Trink ha scritto:
> roberto ha scritto:
>> Trink ha scritto:
>>> Visto che gli hackerognoli se ne inventano una al minuto volevo sapere
> come
>>> controllare a posteriori che gli aggiornamenti installati sono
> effettivamente
>> A posteriori non puoi, a meno di non avere una copia della macchina
>> precedente all'aggiornamento su cui rifare l'aggiornamento *sicuro*
>> da confrontare con l'altra.
>
> Uhmm... pero', ad esempio, non esiste una lista dei pacchetti di aggiornamento
> ufficiali e una lista di quanto installato? In effetti non potrebbe esserci un

SÃ¬, la puoi anche trovare.

> checksum di quanto installato e come doveva essere?

No.
C'Ã¨ la possibilitÃ di avere la lista dei checksum di come dovevano
essere i pacchetti ufficiali, ma dopo l'installazione non hai la

certezza che tutto ciÃ² che resta sulla macchina non sia stato rifatto
ad arte dal software maligno.

L'unica protezione Ã¨ durante l'aggiornamento, e si fa proprio con le
firme crittografiche degli sviluppatori e con il checksum del pacchetto
PRIMA dell'installazione.

> Si potrebbe implementare uno strumento che confronta queste due liste,
> periodicamente, e vedere se tutto e' ok o ci sono differenze.

Se io ti faccio un pacchetto maligno che sostituisce libpincopalla, e tu
lo installi, non ti stupire se dopo, guardando libpincopalla.deb risulti
perfettamente a posto come checksum, anche se libpincopalla sta rubando
tutti i tuoi dati, mandando proposte oscene a tutto il governo e ad un
paio di vescovi, e sta modificando tutti i dati dell'anagrafe della tua
regione. ;-)

Una volta che lasci eseguire un qualcosa di esterno al sistema, e non
controllato, non devi avere piÃ¹ fiducia di quello che ti dice la tua
macchina, che potrebbe essere diventata complice dell'hackeronzolo.

Esistono programmi antirootkit, esistono programmi che verificano la
rispondenza dei checksum tra la situazione precedente e quella nuova,
ma non sono del tutto sicuri in caso di aggiunta di software, dato che
non possono sapere come avrebbe dovuto essere il checksum del nuovo
programma che hai installato, loro si basano proprio sul confronto tra
una situazione nota (e certificata sicura, a torto o a ragione) e una
attuale dubbia.

>>> originali e certificati ubuntu. Di recente, come da mio post precedente,
> non
>>> ho avuto una bella esperienza. Grazie 1000!
>> Hai avuto solo fretta e un pizzico di superficialitï¿½.
>
> Distrazione telefonica, ahime'...
>

No, parlavo del formattone successivo.
Potevi aspettare, ed analizzare cosa era stato installato, e cercare se
c'era un motivo coerente per la mancata firma del pacchetto.

PS: in realtÃ io sono della scuola di: "nel dubbio, incendia".
Una macchina compromessa la reinstallo al volo (grazie, clonezilla),
dopo averne fatto una copia (rigrazie, clonezilla) che analizzerÃ² con
calma per trovare la debolezza sfruttata e prendere provvedimenti.

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

Subject: Re: Controllare a posteriori gli aggiornamenti
Posted by Giovanni on Fri, 29 Jul 2011 12:02:07 GMT
View Forum Message <> Reply to Message

On 07/29/2011 12:44 PM, roberto wrote:
> PS: in realtÃ io sono della scuola di: "nel dubbio, incendia". Una
> macchina compromessa la reinstallo al volo (grazie, clonezilla),
> dopo averne fatto una copia (rigrazie, clonezilla) che analizzerÃ²
> con calma per trovare la debolezza sfruttata e prendere
> provvedimenti.

Windows dependency :-)

Ciao
Giovanni
--
A computer is like an air conditioner,
it stops working when you open Windows.
< http://giovanni.homelinux.net/ >

Subject: Re: Controllare a posteriori gli aggiornamenti
Posted by Alessandro Selli on Fri, 29 Jul 2011 15:40:59 GMT
View Forum Message <> Reply to Message

Giovanni ha scritto:
> On 07/29/2011 12:44 PM, roberto wrote:
>> PS: in realtÃ io sono della scuola di: "nel dubbio, incendia". Una
>> macchina compromessa la reinstallo al volo (grazie, clonezilla),
>> dopo averne fatto una copia (rigrazie, clonezilla) che analizzerÃ²
>> con calma per trovare la debolezza sfruttata e prendere
>> provvedimenti.
>
> Windows dependency :-)

Mi spieghi che c'entra la dipendenza da Windows con il ripristino da un'immagine di una macchina che si sospetta compromessa?

Ciao,

--
Alessandro Selli, http://alessandro.route-add.net
AVVERTENZA: i messaggi inviati a "trappola" non mi arriveranno.
WARNING: messages sent to "trappola" will never reach me.
Chiave PGP/GPG: EC885A8B

Subject: Re: Controllare a posteriori gli aggiornamenti
Posted by Roberto on Fri, 29 Jul 2011 15:54:41 GMT
View Forum Message <> Reply to Message

Alessandro Selli ha scritto:
> Giovanni ha scritto:
>> On 07/29/2011 12:44 PM, roberto wrote:
>>> PS: in realtÃ io sono della scuola di: "nel dubbio, incendia". Una
>>> macchina compromessa la reinstallo al volo (grazie, clonezilla),
>>> dopo averne fatto una copia (rigrazie, clonezilla) che analizzerÃ²
>>> con calma per trovare la debolezza sfruttata e prendere
>>> provvedimenti.
>> Windows dependency :-)
>
> Mi spieghi che c'entra la dipendenza da Windows con il ripristino da
> un'immagine di una macchina che si sospetta compromessa?

--nota di servizio--
Io non vedo il post cui rispondi, adesso cercherÃ² di capire il perchÃ¨.
Ah: il poster ha vinto una riga omaggio su /etc/news/leafnode/filters
tempo fa, ci sarÃƒÂ stato un motivo. ;-)
--\nota di servizio--

Lo viene a dire proprio a me, che nasco informaticamente parlando ben
prima di windows, i primi sistemi multiutente che ho usato erano unix,
posto con debian, sono quindici anni che imperverso su icol* ecc.ecc.?

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

Subject: Re: Controllare a posteriori gli aggiornamenti
Posted by Giovanni on Fri, 29 Jul 2011 16:49:10 GMT
View Forum Message <> Reply to Message

On 07/29/2011 05:40 PM, Alessandro Selli wrote:

>>> PS: in realtÃ io sono della scuola di: "nel dubbio, incendia".
>>> Una macchina compromessa la reinstallo al volo (grazie,
>>> clonezilla), dopo averne fatto una copia (rigrazie, clonezilla)
>>> che analizzerÃ² con calma per trovare la debolezza sfruttata e
>>> prendere provvedimenti.

>> Windows dependency :-)

> Mi spieghi che c'entra la dipendenza da Windows con il ripristino
> da un'immagine di una macchina che si sospetta compromessa?

Io parlo delle distribuzioni con aggiramenti automatici e del
suggerimento di reinstallare tutto. Tipico di Windows!

Ciao
Giovanni
--
  A computer is like an air conditioner,
  it stops working when you open Windows.
  < http://giovanni.homelinux.net/ >

Subject: Re: Controllare a posteriori gli aggiornamenti
Posted by Giovanni on Fri, 29 Jul 2011 16:57:07 GMT
View Forum Message <> Reply to Message

On 07/29/2011 05:54 PM, roberto wrote:

> Lo viene a dire proprio a me, che nasco informaticamente parlando
> ben prima di windows, i primi sistemi multiutente che ho usato
> erano unix, posto con debian, sono quindici anni che imperverso su
> icol* ecc.ecc.?

Anche se stai imperversando sui NG di linux da 15 anni stai suggerendo
di installare tutto, come ogni bravo utente di windows.

Ciao
Giovanni
--
  A computer is like an air conditioner,
  it stops working when you open Windows.
  < http://giovanni.homelinux.net/ >

Subject: Re: Controllare a posteriori gli aggiornamenti

Posted by Enrico 'Henryx' Bianc on Fri, 29 Jul 2011 17:32:08 GMT
View Forum Message <> Reply to Message

Alessandro Selli wrote:

> Mi spieghi che c'entra la dipendenza da Windows con il ripristino da
> un'immagine di una macchina che si sospetta compromessa?

Nulla, per lui un sistemista e` degno di tale titolo solo se utilizza una distribuzione che non abbia un sistema di pacchettizzazione e di aggiornamento automatico (in altre parole, e` un troll slackware)

Enrico

Subject: Re: Controllare a posteriori gli aggiornamenti
Posted by ValeRyo Saeba on Sat, 30 Jul 2011 06:32:42 GMT
View Forum Message <> Reply to Message

"roberto" <rpoggiNOSPAM@softhome.net.invalid> ha scritto nel messaggio news:ohfag8-h1f.ln1@poggirpc.icrsprint.it

> PS: in realtà io sono della scuola di: "nel dubbio, incendia".
> Una macchina compromessa la reinstallo al volo (grazie, clonezilla),
> dopo averne fatto una copia (rigrazie, clonezilla) che analizzerò con
> calma per trovare la debolezza sfruttata e prendere provvedimenti.

Ok, ma almeno prima cerca di capire se davvero c'è stata una compromissione.
In questo caso non si è collegato a www.hakerz.info per scaricare ed installare il pacchetto: se ricordo il post originale, durante un update gli è stata segnalata una firma non corrispondente.
In quel caso il pacchetto gli arrivava da un repository per lui già affidabile, può essere stato un errore di packaging o stavano aggiornando il repository.

--
ValeRyo
XT600 "Katoki Pajama" - http://www.slimmit.com/go.asp?7Y9
GamerTag: http://card.mygamercard.net/IT/nxe/ValeRyo76.png

Subject: Re: Controllare a posteriori gli aggiornamenti
Posted by Giovanni on Sat, 30 Jul 2011 06:53:54 GMT
View Forum Message <> Reply to Message

On 07/29/2011 07:32 PM, Enrico 'Henryx' Bianchi wrote:

>> Mi spieghi che c'entra la dipendenza da Windows con il
>> ripristino da un'immagine di una macchina che si sospetta
>> compromessa?
>
> Nulla, per lui un sistemista e` degno di tale titolo solo se
> utilizza una distribuzione che non abbia un sistema di
> pacchettizzazione e di aggiornamento automatico (in altre parole,
> e` un troll slackware)

Eccolo li il solito sistemista borioso.
Troll siete voi che su un NG dedicato a linux suggerite di formattare
e reinstallare alla windows.

Bel modo di aiutare chi chiede aiuto.

Ciao
Giovanni
--
A computer is like an air conditioner,
it stops working when you open Windows.
< http://giovanni.homelinux.net/ >

Subject: Re: Controllare a posteriori gli aggiornamenti
Posted by Alessandro Selli on Sat, 30 Jul 2011 11:38:00 GMT
View Forum Message <> Reply to Message

Giovanni ha scritto:
> On 07/29/2011 05:40 PM, Alessandro Selli wrote:
>
>>>> PS: in realtÃ io sono della scuola di: "nel dubbio, incendia".
>>>> Una macchina compromessa la reinstallo al volo (grazie,
>>>> clonezilla), dopo averne fatto una copia (rigrazie, clonezilla)
>>>> che analizzerÃ² con calma per trovare la debolezza sfruttata e
>>>> prendere provvedimenti.
>
>>> Windows dependency :-)
>
>> Mi spieghi che c'entra la dipendenza da Windows con il ripristino
>> da un'immagine di una macchina che si sospetta compromessa?
>
> Io parlo delle distribuzioni con aggiramenti automatici e del
> suggerimento di reinstallare tutto. Tipico di Windows!

Che non c'entra nulla con quello che aveva scritto roberto, che
riguardava il ripristino da un'immagine di una macchina che si sospetta
compromessa.

Che c'entra Windows e il bisogno di formattare e reinstallare un sistema?

Ciao,

--
Alessandro Selli http://alessandro.route-add.net
AVVERTENZA: i messaggi inviati a "trappola" non mi arriveranno.
WARNING: messages sent to "trappola" will never reach me.

Subject: Re: Controllare a posteriori gli aggiornamenti
Posted by Roberto on Mon, 01 Aug 2011 09:32:45 GMT
View Forum Message <> Reply to Message

ValeRyo Saeba ha scritto:
> "roberto" <rpoggiNOSPAM@softhome.net.invalid> ha scritto nel messaggio
> news:ohfag8-h1f.ln1@poggirpc.icrsprint.it
>
>> PS: in realtÃ io sono della scuola di: "nel dubbio, incendia".
>> Una macchina compromessa la reinstallo al volo (grazie, clonezilla),
>> dopo averne fatto una copia (rigrazie, clonezilla) che analizzerÃ² con
>> calma per trovare la debolezza sfruttata e prendere provvedimenti.
>
> Ok, ma almeno prima cerca di capire se davvero c'Ã¨ stata
> una compromissione.
> In questo caso non si Ã¨ collegato a www.hakerz.info per scaricare
> ed installare il pacchetto: se ricordo il post originale, durante un
> update gli Ã¨ stata segnalata una firma non corrispondente.

Esatto. Riassunto delle puntate precedenti:

Visto la vaghezza del post iniziale, io avevo mandato una risposta
per cui mi aspettavo dettagli, per poi arrivare alle tue stesse
conclusioni, ma l'OP non ha aspettato nulla, ed ha riformattato e
reinstallato tutto, prima di leggere qualsiasi risposta.

Dopo, seguendo la piÃ¹ classica teoria della deriva degli argomenti,
siamo passati a disquisizioni teorico tecniche sul da farsi in caso
di effettivo dubbio, se Ã¨ riconoscibile un pacchetto possibilmente
maligno *dopo* l'installazione, e siamo arrivato alla mia mania
windowsesca (dice giovanni) di rasare al volo una macchina che con
buona probabilitÃ so essere stata compromessa, per riattivare al
piÃ¹ presto i servizi e poi analizzare post mortem il reperto.

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