
Keylogger: come funzionano e come identificarli

Parte 1

- I keylogger
- Perché i keylogger rappresentano un pericolo
- Come vengono utilizzati dai criminali della rete
- Aumento dell'uso dei keylogger
- Come si costruiscono i keylogger
- Come si diffondono i keylogger
- Protezione contro i keylogger
- Conclusioni

Keylogger: come funzionano e come identificarli

A febbraio 2005 Joe Lopez, un uomo d'affari della Florida, mosse un'azione legale contro la Bank of America dopo che degli hacker sconosciuti avevano rubato 90,000 dollari americani dal suo conto della Bank of America. I soldi erano stati trasferiti in Lettonia.

(http://searchsecurity.techtargget.com/columnItem/0,294698,sid14_gci1062440,00.html)

Un'indagine dimostrò che il computer di Mr Lopez era stato infettato da un programma maligno, Backdoor.Coreflood, che registra ogni battuta sulla tastiera e invia queste informazioni via Internet. In questa maniera gli hacker entrarono in possesso della user name e della password di Joe Lopez, visto che Mr Lopez aveva utilizzato spesso Internet per gestire il proprio conto sulla Bank of America.

Tuttavia, la Corte non deliberò in favore della vittima, dichiarando che Mr Lopez non aveva preso alcun tipo di precauzione di base nel gestire su Internet il suo conto bancario. Infatti, la segnalazione del codice maligno trovato all'interno del suo sistema, era stata aggiunta in quasi tutti i database di prodotti antivirus già nel 2003.

La perdita di denaro da parte di Joe Lopez era stata causata dalla sua noncuranza e da un programma ordinario di keylogging.

I keylogger

Il termine "keylogger" è un termine neutrale, la parola descrive la funzione del programma. La maggior parte delle fonti definiscono un keylogger come un programma software ideato per monitorare tutte le battute che vengono effettuate sulla tastiera di un computer.

Alcuni programmi legittimi possono prevedere una funzione di keylogging, ad esempio per l'utilizzo di alcune funzioni di un programma mediante l'uso dei "hotkey". Ci sono molti software legittimi creati per consentire agli amministratori di tenere traccia di quello che i lavoratori fanno durante il giorno, o per consentire agli utenti di tenere traccia delle attività effettuate da terzi sui loro computer. Comunque, il confine etico tra monitoraggio giustificato e spionaggio è alquanto sottile. I software legittimi spesso sono utilizzati deliberatamente per rubare all'utente informazioni confidenziali come le password.

La maggior parte dei keylogger odierni sono considerati software o hardware legittimi e sono venduti sul mercato aperto. Gli sviluppatori e i venditori offrono una lunga lista di casi nei quali sarebbe del tutto legale e consono utilizzare i keylogger:

- Controllo da parte dei genitori: i genitori possono tenere traccia di quello che fanno i loro figli su Internet e possono scegliere di essere avvisati se ci sono dei tentativi di entrare nei siti web che contengono contenuti per adulti o in qualche modo inappropriati
- Le mogli gelose o i partner possono utilizzare i keylogger per tenere traccia delle azioni effettuate su Internet dalle loro dolci metà se sospettano "tradimenti virtuali"
- Sicurezza nelle società: tenendo traccia dell'uso dei computer nel caso di attività non relative al lavoro o nel caso di uso delle postazioni dopo le ore lavorative
- Sicurezza nelle società: per tenere traccia dei caratteri e delle parole chiave e delle frasi associate con informazioni commerciali che potrebbero danneggiare la società (materialmente o in altro modo) se divulgate
- Per altri tipi di sicurezza (per attuazione della legge): usare quanto documentato nei keylogger per analizzare e tenere traccia degli incidenti legati all'uso dei personal computer
- Altri motivi.

Comunque, le giustificazioni indicate sopra sono più soggettive che oggettive; tutte le situazioni descritte possono esser risolte usando altri metodi. In più, ogni programma di keylogging legittimo

Keylogger: come funzionano e come identificarli

può sempre esser utilizzato per un intento maligno o criminale. Oggi, i keylogger sono usati soprattutto per rubare agli utenti informazioni relative a diversi sistemi di pagamento on-line, tanto che gli scrittori di virus scrivono continuamente nuovi Trojan keylogger per questo preciso scopo.

Per di più, molti keylogger si nascondono all'interno del sistema (ad esempio hanno funzionalità rootkit) che li fa apparire come dei programmi Trojan veri e propri.

Da quando tali programmi hanno cominciato ad essere utilizzati dai criminali della rete, la loro individuazione è diventata una priorità per le società antivirus. Il sistema di classificazione dei malware di Kaspersky Antivirus enumera una categoria ad hoc per i programmi maligni con funzionalità di keylogging: Trojan-Spy (<http://www.viruslist.com/ru/viruses/encyclopedia?chapter=156769330#trojan-spy>). I programmi Trojan-Spy, come suggerito dal loro nome, tengono traccia dell'attività dell'utente, salvano le informazioni nell'hard disk dell'utente e poi le inoltrano all'autore o all'utilizzatore del Trojan. Le informazioni raccolte includono le battute sulla tastiera e le schermate, utilizzate per rubare informazioni bancarie, aiutando così le frodi on-line.

Perché i keylogger rappresentano un pericolo

A differenza di altri tipi di programmi maligni, i keylogger non rappresentano alcun pericolo per il sistema in se stesso. Tuttavia, questi possono portare un grave pericolo per gli utenti, in quanto possono essere usati per intercettare password ed altre informazioni confidenziali inserite attraverso la tastiera del computer. Come conseguenza, i criminali della rete possono appropriarsi di codici PIN e numeri di conto per sistemi di pagamenti on-line, password per conti di giochi on-line, indirizzi e-mail, user name, e-mail password, etc.

Una volta che un criminale della rete si è impossessato di informazioni confidenziali dell'utente, può trasferire denaro dal conto dell'utente o accedere ai conti dei siti di giochi on-line. Sfortunatamente, l'accesso a informazioni confidenziali può alle volte portare a conseguenze ben più serie che ad una perdita di qualche dollaro. I keylogger possono essere utilizzati come strumenti per spionaggio industriale e politico, attraverso l'accesso a informazioni che possono contenere dati commerciali di proprietà e materiale che potrebbe compromettere la sicurezza di organizzazioni commerciali e statali (per esempio, rubando chiavi private codificate).

I keylogger, il phishing e il social engineering (guarda *Computers, Networks and Theft*: <http://www.viruslist.com/en/analysis?pubid=202913259>) rappresentano oggi i principali metodi utilizzati per le frodi in rete. Gli utenti che sono a conoscenza dei problemi di sicurezza possono facilmente proteggersi contro il phishing ignorando le e-mail sospette e non inserendo alcuna informazione personale all'interno di siti web a cui le email indirizzano. Comunque, per gli utenti è molto più difficile combattere i keylogger: l'unico metodo possibile è quello di usare una soluzione di sicurezza appropriata, anche se di solito risulta impossibile per l'utente capire che è stato installato un keylogger all'interno della sua macchina.

Secondo Cristine Hoepers (<http://www.nytimes.com/2006/02/27/technology/27hack.html>), manager del Computer Emergency Response Team del Brasile per la Commissione di Guida di Internet, i keylogger hanno tolto il phishing dal primo posto nella classifica dei metodi più utilizzati per rubare informazioni confidenziali. Inoltre, i keylogger stanno diventando sempre più sofisticati in quanto tengono traccia dei siti web visitati dall'utente e registrano soltanto le battute della tastiera per entrare nei siti web di particolare interesse per i criminali della rete.

Negli anni recenti abbiamo assistito ad un considerevole aumento nel numero di diversi tipi di programmi maligni che possiedono delle funzionalità di keylogging. Nessun utente Internet è immune dai criminali della rete, non importa in che parte del mondo sia e in quale organizzazione lavori.

Come vengono utilizzati i keylogger dai criminali della rete

Uno dei casi di keylogging più famosi è stato il furto di 1 milione di dollari americani dai conti di clienti della banca scandinava Nordea

Keylogger: come funzionano e come identificarli

(<http://news.zdnet.co.uk/security/0,1000000189,39285547,00.htm>). Ad agosto 2006 i clienti di Nordea cominciarono a ricevere delle e-mail che sembravano provenire dalla banca in cui si suggeriva di installare un certo prodotto antispam che era allegato al messaggio. Una volta che l'utente apriva il file e lo scaricava sul suo computer e la macchina si infettava con il conosciuto Trojan chiamato Haxdoor. Questo veniva attivato ogni qualvolta la vittima si registrava ai servizi online e il Trojan mostrava una notifica di errore con la richiesta di inserire di nuovo le informazioni di registrazione. Il keylogger incorporato nel Trojan registrava le informazioni inserite dai clienti della banca e dopo inviava queste informazioni ai server dei criminali della rete. In questa maniera i criminali della rete riuscirono ad accedere ai conti dei clienti trasferendo denaro dagli stessi conti. Secondo quanto dichiarato dall'autore dell'Haxdoor, il Trojan era stato anche utilizzato per alcuni attacchi contro banche australiane e molte altre.

Il 24 gennaio 2004 il noto worm Mydoom (http://www.infoworld.com/article/04/01/27/HNdoomworm_1.html) causò una vasta infezione. Mydoom superò il record stabilito in precedenza da Sobig, provocando la più grande infezione Internet della storia. Il worm utilizzava metodi di social engineering e un attacco DoS su www.sco.com; come conseguenza il sito diventava irraggiungibile o instabile per alcuni mesi. Il worm lasciò un Trojan sui computer infettati che fu in seguito usato per infettare le macchine delle vittime con nuove modificazioni del worm. Non venne pubblicizzato sui media il fatto che Mydoom aveva una funzione keylogging di raccolta dei numeri delle carte di credito.

All'inizio del 2005 la polizia di Londra impedì un tentativo di rubare informazioni bancarie (http://news.bbc.co.uk/2/hi/uk_news/4356661.stm). Dopo aver attaccato un sistema bancario, i criminali avevano pianificato di rubare 423 milioni di dollari americani dagli uffici di Londra della Sumitomo Mitsui. Il componente principale del Trojan usato, inventato dal 32enne Yeron Bolondi, fu un keylogger che permetteva ai criminali della rete di tenere traccia di tutte le battute della tastiera effettuate ogni volta che le vittime utilizzavano il sito della banca.

A maggio 2005 a Londra la polizia di Israele arrestò una coppia sposata accusata di aver sviluppato programmi maligni usati da alcune compagnie israeliane per **spionaggio industriale** (<http://www.washingtonpost.com/wp-dyn/content/article/2005/05/30/AR2005053000486.html>). Le dimensioni dell'attività di spionaggio compiuta fu scioccante: le compagnie nominate dalle autorità israeliane all'interno dei rapporti investigativi includevano fornitori di telefoni cellulari come Cellcom e Pelephone e YES, provider televisivo satellitare. Secondo quanto scritto nel rapporto, il Trojan era stato utilizzato per accedere a informazioni relative all'agenzia PR Rani Rahav, tra i cui clienti figurava la Partner Communication (il secondo più importante provider di telefoni cellulari in Israele) e il gruppo della televisione via cavo HOT. La società Mayer, che importa in Israele le macchine della Volvo e della Honda fu sospettata di aver commesso attività di spionaggio industriale contro Champion Motors, che importa nel paese macchine Audi e Volkswagen. Ruth Brier-Haephtrati, che aveva venduto il Trojan keylogging creato da suo marito Michael Haephtrati, fu condannata a 4 anni di prigione mentre Michael a 2 anni.

A febbraio 2006, la polizia brasiliana arrestò 55 persone coinvolte nella diffusione di programmi maligni usati per rubare informazioni e password all'interno di sistemi bancari. (<http://www.nytimes.com/2006/02/27/technology/27hack.html?pagewanted=2&ei=5088&en=b794c1adbbd71162&ex=1298696400>). Ogni volta che gli utenti visitavano i siti delle loro banche, i keylogger venivano attivati, tenendo traccia e inviando tutte le informazioni inserite in quelle pagine. Il totale dei soldi rubati da 200 conti di clienti di sei banche del paese fu di 4.7 milioni di dollari americani.

Più o meno nello stesso periodo, fu arrestato un gruppo di giovani criminali (20-30 anni) russi e ucraini. Alla fine del 2004, il gruppo aveva incominciato ad inviare ai clienti di banche in Francia e ad un numero di altri paesi dei messaggi e-mail che contenevano un programma maligno, ossia un keylogger. Inoltre, questi programmi spia furono installati all'interno di siti web creati appositamente; gli utenti furono spinti ad andare su questi siti usando classici metodi di social engineering. Nella stessa maniera utilizzata nei casi descritti sopra, il programma si attivava ogni volta che gli utenti visitavano i siti web delle loro banche e raccoglieva tutte le informazioni inserite dall'utente e le inviava ai criminali della rete. Nel giro di 11 mesi furono rubati oltre 1 milione di dollari americani. (<http://www.guardian.co.uk/france/story/0,,1703777,00.html>).

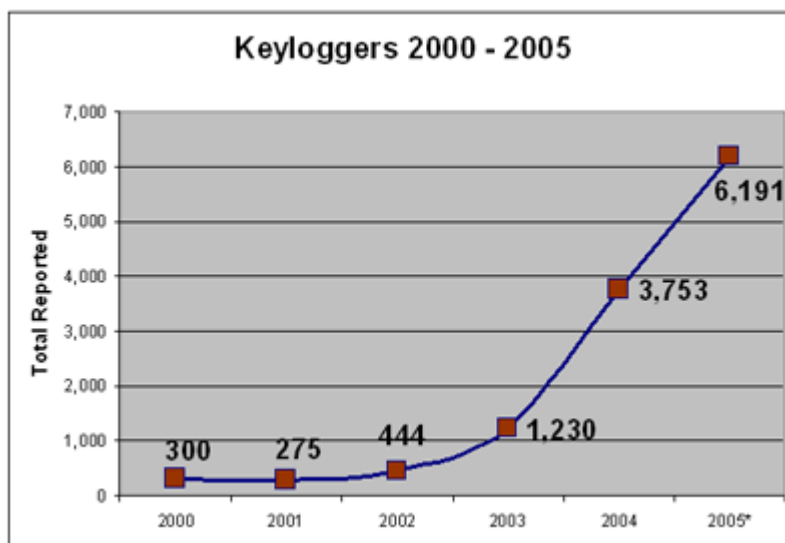
Keylogger: come funzionano e come identificarli

Ci sono molti altri esempi di criminali che utilizzano keylogger, in quanto questi programmi rappresentano ad oggi i dispositivi più affidabili per tenere traccia delle informazioni elettroniche.

Aumento dell'uso di keylogger da parte dei criminali della rete

Il fatto che i criminali sempre più spesso scelgano di usare i keylogger è confermato anche dalle compagnie di sicurezza IT.

Uno dei recenti rapporti di VeriSign (http://www.verisign.com/verisign-inc/news-and-events/news-archive/us-news-2005/page_036258.html) sottolinea come in questi ultimi anni la compagnia si sia registrata una rapida crescita del numero di programmi maligni con funzionalità di keylogging.



Fonte: iDefense, una società VeriSign

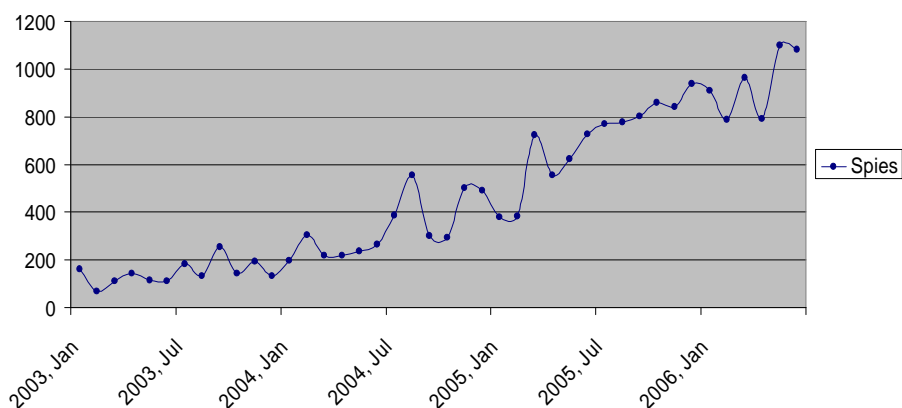
Un rapporto pubblicato da Symantec mostra che quasi il 50% dei programmi maligni identificati dagli analisti della società durante l'anno scorso non minacciano direttamente i computer ma sono utilizzati dai criminali della rete per la raccolta di informazioni personali dell'utente.

In base a quanto stabilito da una ricerca condotta da John Bambenek, un analista del SANS Institute (<http://handlers.dshield.org/jbambenek/keylogger.html>), circa 10 milioni di computer solo negli USA sono attualmente infettati con programmi maligni che possiedono una funzione di keylogging. Utilizzando questi dati, insieme al numero totale degli utenti americani di sistemi di pagamento on-line, si stima che l'ammontare totale di possibili perdite possa raggiungere i 24.3 milioni di dollari americani.

Kaspersky Lab identifica costantemente i nuovi programmi maligni che hanno funzioni di keylogging. Uno dei primi allarmi di tali virus su www.viruslist.com, sito di Kaspersky Lab, dedicato a dare informazioni sui malware, fu pubblicato il 15 giugno 2001. La minaccia riguardava TROJ_LATINUS:SVR, un trojan che possedeva una funzione di keylogging. Da allora si è assistito ad un flusso regolare di nuovi keylogger e nuove modificazioni. Attualmente il database antivirus di Kaspersky contiene più di 300 famiglie di keylogger. Questo numero non comprende i keylogger che sono parte di minacce più complesse (ad esempio quelli in cui il componente spia è dotato di ulteriori funzionalità).

Molti dei nuovi programmi maligni sono degli ibridi che implementano molte tecnologie diverse. Per questo motivo, ogni categoria di programma maligno può includere programmi con subfunzionalità di keylogger. Il grafico sotto mostra l'aumento nel numero dei programmi spia identificati da Kaspersky Lab ogni mese. Molti di questi programmi usano la tecnologia di keylogging.

Keylogger: come funzionano e come identificarli



Come si costruiscono i keylogger

L'idea principale che sta dietro ai keylogger è quella di mettersi in mezzo a due link nella catena di due eventi, ogni volta che un tasto viene premuto e ogni volta che le informazioni circa quella battuta della tastiera viene mostrata nel monitor.

L'esperienza dimostra che, quanto più complesso è il tentativo di attacco, tanto meno viene utilizzato nei programmi trojan comuni, per essere invece utilizzato per rubare dati finanziari da una vittima specifica.

I keylogger possono essere divisi in due categorie: **dispositivi di keylogging** e **software di keylogging**. I keylogger che rientrano all'interno della prima categoria di solito sono piccoli dispositivi che possono essere collegati alla tastiera oppure posizionati all'interno di un cavo o dello stesso computer. La categoria dei software di keylogging è fatta da programmi speciali creati per tenere traccia e registrare le battute dei tasti.

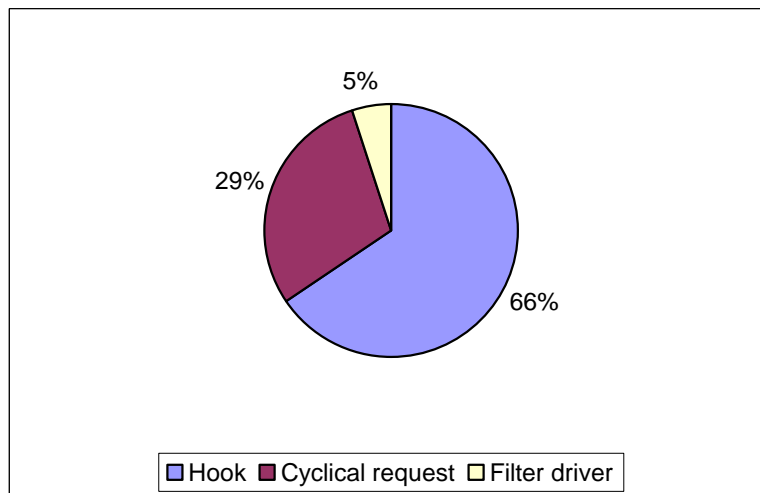
Questi i metodi più comuni usati per costruire software di keylogging:

- Un sistema di gancio che intercetta la notifica che un tasto è stato schiacciato (istallato usando WinAPI SetWindowsHook per i messaggi inviati con la procedura Window. La maggior parte delle volte è scritto in C)
- Una richiesta di informazioni cicliche sulla tastiera da parte della stessa tastiera (usando WinAPI Get(Async)KeyState o GetKeyboardState – molto spesso scritta in Visual Basic, qualche volta in Borland Delphi);
- Usando un driver di filtro (richiede una conoscenza specifica ed è scritto in C).

Nella seconda metà di questo articolo, che sarà pubblicata a breve, verrà data una spiegazione dettagliata delle diverse maniere in cui vengono costruiti i keylogger. Prima però ecco alcune statistiche.

Il grafico a torta qui sotto mostra una brusca interruzione dei diversi tipi di keylogger:

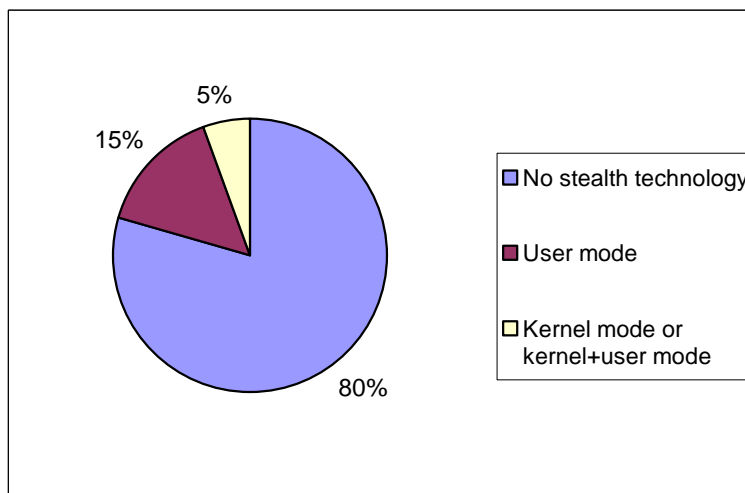
Keylogger: come funzionano e come identificarli



Di recente, sono diventati assai numerosi i keylogger che camuffano i loro file per evitare di essere scoperti manualmente o da un programma antivirus. Queste tecniche di cautela sono chiamate tecnologie rootkit. Ci sono due principali tecnologie rootkit usate dai keylogger

- Camuffarsi **in modalità user**
- Camuffarsi **in modalità guscio**

Il grafico a torta qui sotto mostra una brusca interruzione delle tecniche utilizzate dai keylogger per mascherare la loro attività



Come si diffondono i keylogger

I keylogger si diffondono quasi alla stessa maniera di tutti gli altri programmi maligni. Se si escludono i casi in cui i keylogger sono acquistati e installati da mogli o partner gelose e i casi di keylogger usati per servizi di sicurezza, i keylogger si diffondono soprattutto nei seguenti metodi:

- Un keylogger può essere installato quando un utente apre un file allegato ad una e-mail
- Un keylogger può essere installato quando un file viene lanciato da una directory ad accesso aperto su un network P2P

Keylogger: come funzionano e come identificarli

- Un keylogger può essere installato attraverso uno script di una pagina web che sfrutta una vulnerabilità del browser. Il programma sarà lanciato automaticamente quando l'utente visiterà il sito infetto
- Un keylogger può essere installato in un altro programma maligno già presente nella macchina della vittima, nel caso in cui il programma stesso sia capace di scaricare ed installare altri malware all'interno del sistema

Come proteggersi dai keylogger

La maggior parte delle società di antivirus hanno già provveduto ad aggiungere nei loro database i keylogger conosciuti, offrendo una protezione contro i keylogger non diversa da quella offerta per proteggersi da altri tipi di programmi maligni: attraverso l'installazione di un prodotto antivirus e aggiornando il database. Tuttavia, poiché la maggior parte dei prodotti antivirus classificano i keylogger come *programmi potenzialmente maligni o potenzialmente indesiderabili*, gli utenti devono assicurarsi che il loro prodotto antivirus identifichi questo tipo di malware attraverso delle applicazioni di default. Altrimenti il prodotto dovrebbe essere configurato, per assicurare una protezione contro i più comuni keylogger.

Conviene guardare più da vicino i metodi che si possono usare per proteggersi contro keylogger sconosciuti o contro un keylogger creato per colpire uno specifico sistema.

Poiché il proposito principale dei keylogger è quello di acquisire informazioni confidenziali (numeri di carte bancarie, password, etc.), le maniere più logiche di proteggersi contro keylogger sconosciuti sono:

1. usare password utilizzabili soltanto una volta (password irripetibili) o doppie autenticazioni
2. usare un sistema che possiede una protezione proattiva creata per identificare i software di keylogging,
3. usare una tastiera virtuale.

L'adozione di password che possono usarsi solo una volta aiuta a diminuire la perdita nel caso in cui la password viene intercettata, in quanto la stessa può usarsi solo una volta e il suo periodo di utilizzo è limitato. Anche se viene intercettata una di queste password, un criminale delle rete non sarà capace di usarla per ottenere accesso a informazioni confidenziali.

Per avere delle password irripetibili, si possono utilizzare degli speciali dispositivi come:

1. una chiave USB (come Aladdin eToken NG OTP - http://www.aladdin.ru/catalog/etoken/public_detail.php?ID=5630):



immagine presa dal sito web: <http://www.aladdin.ru>

2. un "calcolatore" (come RSA SecurID 900 Signing Token - <http://www.rsa.com/node.aspx?id=1158>):



Keylogger: come funzionano e come identificarli

Immagine presa dal sito web: <http://www.rsa.com>

Per creare delle password irripetibili si possono utilizzare anche sistemi di messaggi di testo di telefoni cellulari, registrati con il sistema bancario, e ricevere come risposta un codice PIN. Il PIN viene quindi usato insieme al codice personale per l'autenticazione.

Nel caso in cui uno degli apparecchi sopra indicati venga usato per creare delle password irripetibili, questo sarà il procedimento utilizzato:

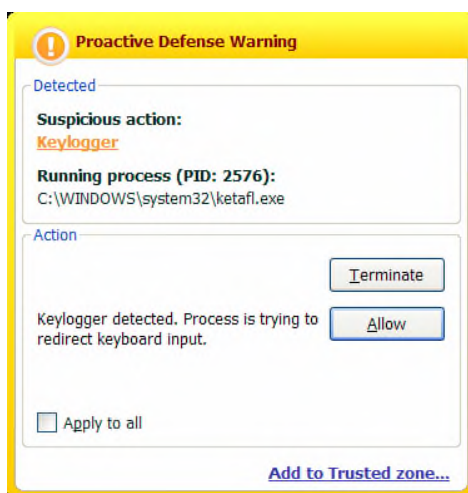
1. l'utente si connette a Internet e apre una finestra di dialogo dove vanno inserite le informazioni personali
2. successivamente schiaccia un bottone sul dispositivo per creare una password irripetibile, per 15 secondi apparirà una password sul display LDC del dispositivo
3. l'utente inserirà nella finestra di dialogo la sua user name , il codice PIN e la password irripetibile generata (di solito il codice PIN e la chiave sono inseriti una dopo l'altra nei rispettivi campi)
4. i codici inseriti vengono verificati dal server che decide se l'utente può accedere o meno alle informazioni confidenziali

quando si usa un dispositivo per generare una password l'utente inserirà il suo codice PIN sulla tastiera e schiaccerà il bottone ">" .

I generatori di password irripetibili sono largamente usati dai sistemi bancari in Europa, Asia, USA e Australia. Ad esempio, Lloyds TSB, una banca tra le più importanti, ha deciso di utilizzare dei generatori di password già a partire da novembre del 2005 (<http://news.bbc.co.uk/1/hi/business/4340898.stm>).

In questo caso, tuttavia, la compagnia ha dovuto spendere una somma considerevole di denaro in quanto ha dovuto comprare e distribuire i generatori di password ai suoi clienti e sviluppare/comprare i software di accompagnamento.

Una soluzione a costo minore è rappresentata dalla protezione proattiva da parte del cliente, la quale può allertare un utente ogni volta in cui viene fatto un tentativo di installare dei software di keylogging.



Protezione proattiva contro keylogger di Kaspersky Internet Security

Il principale svantaggio di questo metodo è dato dal fatto che l'utente è coinvolto attivamente e deve decidere quale azione intraprendere. Se non è un utente con molta conoscenza tecnica, potrebbe prendere la decisione sbagliata, con il risultato di consentire ad un keylogger di bypassare la soluzione antivirus. Tuttavia, se gli sviluppatori minimizzano il coinvolgimento dell'utente, allora i keylogger saranno in grado di evitare di essere identificati grazie ad una policy di sicurezza non

Keylogger: come funzionano e come identificarli

abbastanza rigorosa. Tuttavia, se le applicazioni sono troppo rigorose, potrebbero essere bloccate anche altre utili programmi che contengono funzioni legittimate di keylogging.

L'ultimo metodo che potrebbe essere usato per proteggersi contro i software di keylogging e gli hardware è quello di utilizzare una tastiera virtuale. Questo è un programma che mostra una tastiera sullo schermo e permette di premere i tasti usando il mouse.

L'idea di una tastiera su sul display del computer non è una novità, il sistema operativo Windows possiede già una tastiera sul display che può essere lanciata facendo: Start > Programmi > Accessori > Accessibilità > tastiera sul display



Esempio di una tastiera sul display nel sistema operativo Windows

Comunque, le tastiere sul display non sono un metodo molto popolare per sconfiggere i keylogger. Non sono state inventate come protezione contro i pericoli della rete ma come un dispositivo di accesso per gli utenti disabili. Le informazioni inserite utilizzando le tastiere sul display possono essere intercettate facilmente da un programma maligno. Per poterle utilizzare come protezione contro i keylogger, queste devono essere ideate in maniera tale da assicurare che le informazioni inserite o trasmesse tramite di esse non possano essere intercettate.

Conclusioni

Questo articolo ha fornito un quadro generale su come funzionano e come vengono usati i keylogger, siano essi software o hardware di keylogging.

- Anche se gli sviluppatori di keylogger immettono sul mercato i loro prodotti come dei software legittimi, la maggior parte dei keylogger possono essere utilizzati per rubare informazioni personali e per attività di spionaggio sia politico che industriale.
- Ad oggi, i keylogger, insieme ai metodi phishing e a quelli di social engineering, sono uno dei metodi più comunemente utilizzati per le frodi in rete
- Le società di sicurezza IT hanno registrato un regolare aumento nel numero di programmi maligni che possiedono delle funzionalità di keylogging
- I rapporti mostrano come ci sia un aumento nella tendenza ad utilizzare le tecnologie rookit nei software di keylogging, per aiutare i keylogger a evadere una possibile identificazione manuale o da parte di soluzioni antivirus
- Solo delle protezioni ad hoc possono identificare se un keylogger viene utilizzato per propositi di spionaggio
- Queste le misure che si possono prendere per proteggersi dai keylogger:
 - Usare un antivirus standard che può essere adattato per identificare potenziali software maligni (impostazioni di default per molti prodotti)
 - Una protezione proattiva riuscirà a proteggere il sistema contro nuovi keylogger o modificazioni di keylogger esistenti
 - Usare una tastiera virtuale o un sistema per generare delle password irripetibili per proteggersi contro software e hardware di keylogging.