# I KEYLOGGERS

**SEMINARIO PRESENTATO DA**

**QUERCINI GIANLUCA**

**1999S014@educ.disi.unige.it**

# I KEYLOGGERS

I keyloggers sono strumenti in grado di intercettare e memorizzare ogni tasto battuto sulla tastiera del PC. Normalmente quando si parla di keylogger, si intendono strumenti software, ma è bene sapere che sul mercato sono presenti anche dei dispositivi hardware atti a questo scopo e che in questo campo l'hardware costituisce una novità. Ad esempio la KeyGhost, una società neozelandese, produce due dispositivi keyloggers: il KeyGhost Device e il KeyGhost Security Keyboard. Il primo è un cavo molto sottile (fatto apposta in modo che l'utente della macchina su cui è installato non lo noti) che è collegato alla tastiera e che registra in una sua memoria interna ogni carattere digitato dall'utente. La memoria interna ha una capacità di 2 MB, cioè una memoria sufficiente per memorizzare la quantità di tasti che si possono digitare in un anno intero. Inoltre il dispositivo funziona con qualunque sistema operativo e non ha bisogno di drivers per il suo funzionamento. La seguente figura mostra il dispositivo evidenziato in giallo:

Il secondo dispositivo, invece, è una tastiera che contiene al suo interno un dispositivo che intercetta i tasti premuti e li memorizza in una memoria interna anch'essa di 2 MB. In questo caso per l'utente di una macchina accorgersi della presenza di un dispositivo keylogger risulta pressoché impossibile. E' anche possibile modificare opportunamente le normali tastiere per dotarle di un keylogger al loro interno.
Una volta che la memoria interna si satura, il dispositivo continua a lavorare, soprascrivendo i dati precedentemente memorizzati. Per potere leggere i dati in memoria, l'utente deve aprire un qualunque wordprocessor (come Word o Notepad) e digitare uno speciale codice chiamato PUC (Personal Unlock Code). Il dispositivo riconosce il codice e apre il menu seguente:

*Menu>*

1) *Entire Log Download [**get entire log**]*
2) *Section Log Download [**get part of log**]*
3) *Wipe Log [**Erase Log Quickly**]*
4) *Format Memory [**securely erase log**]*

A questo punto l'utente sceglie l'opzione da lui desiderata e tutto ciò che è presente sulla memoria può anche essere salvato in un file per eventuali successive consultazioni.

I keyloggers intesi come software sono in circolazione già da parecchi anni (anni '80), anche se agli inizi si trattava di programmi molto rudimentali in grado solo di memorizzare i tasti premuti dall'utente in un file di testo, detto file di log. Oggi, invece, la maggior parte dei keyloggers in commercio prevede la configurazione di numerose opzioni. Una delle più importanti è la possibilità di specificare un indirizzo e-mail o un server web a cui inviare periodicamente il file di log, in modo che colui che ha installato un keylogger su una macchina possa anche leggere ciò che l'utente della macchina ha scritto con la sua tastiera. Tali programmi sono a tutti gli effetti considerati spyware, e non già come virus. Infatti un virus ha come suo scopo la sua diffusione ad altre macchine e la modifica o distruzione dei dati presenti sulla macchina in cui risiede. Il keylogger non ha questo scopo. Si deve altresì dire che le due entità non sono tra loro indipendenti. Un virus, infatti, può essere il vettore di un keylogger e testimone di ciò è l'ormai famoso virus BugBear.
Cercando con un qualsiasi motore di ricerca, è facile imbattersi in decine di siti web che offrono il download di keyloggers, e questo può a prima vista sembrare strano, se si pensa a quali impatti negativi abbiano questi programmi sulla sicurezza. Ma i keyloggers non sono solo usati dagli hackers per catturare informazioni confidenziali quali passwords, numeri di carta di credito, e-mail e quant'altro, ma anche, ad esempio, da genitori che intendono controllare le conversazioni dei propri figli in chat, da mariti gelosi che vogliono controllare la propria moglie e anche da datori di lavoro per controllare che i dipendenti facciano buon uso delle risorse dell'azienda. Ed infatti la maggior parte dei prodotti che si trovano in rete sono pubblicizzati proprio rivolgendosi a queste categorie di persone. Anche se spesso e volentieri sono i malintenzionati a usufruire di questa tecnologia. Ma a conferma del fatto che un keylogger può essere usato allo scopo di difesa della sicurezza e non di attacco alla sicurezza, citiamo il famoso (negli Stati Uniti) caso Scarfo, figlio di un potente boss della Cosa Nostra di Philadelphia. Durante una irruzione dell' FBI nell'ufficio dove Scarfo lavorava, gli investigatori hanno installato sul suo PC un cavo simile a quello visto prima. In questo modo sono riusciti a catturare la chiave di cifratura che veniva usata per cifrare alcuni dati molto riservati. E questi dati riservati aiutarono l' FBI ad incriminare il boss. L'uso di tali tecniche furono ovviamente contestate dai legali di Scarfo, ma alla fine i giudici ritennero valide le prove offerte dalla pubblica accusa

grazie al keylogger. E questo è stato il primo caso di uso di un keylogger nelle attività investigative.
Dal punto di vista tecnico, i keyloggers sono costituiti generalmente da un unico file eseguibile e non necessitano di nessuna installazione. Un attaccante ha vari modi per installare un keylogger su una macchina: direttamente, se ha accesso fisico alla macchina, oppure facendo pervenire all'utente (o agli utenti) della macchina un floppy o un cd-rom contenente l'applicazione e convincendoli ad installarla. Oppure l'attaccante ha anche la possibilità di sferrare un attacco remotamente e servirsi di un Troyan per fare pervenire il keylogger a destinazione e di solito questa è la strada seguita. Una volta installato, il programma di solito va in esecuzione all'avvio del sistema operativo (anche se molti keylogger oggi in commercio prevedono la possibilità di controllare il momento in cui avviare l'attività di monitoraggio) e memorizza le digitazioni dell'utente in un file di log. Un buon keylogger a questo punto deve potere riuscire a rimanere invisibile all'utente per il periodo più lungo possibile. Per fare questo quindi non deve comparire nella lista dei processi running (cioè non deve potere essere visibile quando l'utente digita CTRL-ALT-CANC su un sistema windows o ps su un sistema Linux) e non deve nemmeno lasciare tracce ad esempio icone nel menu avvio. Un altro elemento che deve rimanere ben nascosto è il file di log. Solitamente viene posizionato in una directory molto "affollata", in modo che l'utente non lo possa notare, e gli viene dato un nome poco significativo, in modo da non richiamare l'attenzione su di sé. Oppure viene messo in una directory di sistema (per esempio in c:\windows) che generalmente contiene tanti file e viene visitata poco spesso dall'utente medio. Inoltre l'utente di solito è restio a cancellare files da queste directory per paura di cancellare files necessari per il funzionamento delle applicazioni da lui installate o del sistema operativo. Per aumentare la sua invisibilità il file di log può anche essere criptato. In questo modo, anche se l'utente (per sbaglio, o per caso) dovesse aprire il file, non potrebbe capire se è un file sospetto.
A questo punto l'attaccante deve poter riuscire a leggere il log (altrimenti avrebbe sprecato fatica!). E ha due sole alternative: leggerlo direttamente sulla macchina dove risiede approfittando dell'assenza dell'utente (come potrebbe fare un genitore quando il proprio figlio è a scuola oppure un marito geloso…), con il rischio di essere sorpreso proprio dall'utente stesso, oppure leggerlo remotamente. Come? Come detto prima, la maggior parte dei keyloggers in circolazione prevede la possibilità di specificare un indirizzo e-mail o un server web a cui mandare il file di log. A questo punto l'attaccante può leggere il log con tutta calma. Attenzione che anche questo secondo metodo comporta dei rischi. In questo caso è vero che l'attaccante è comodamente seduto a casa sua e non può essere sorpreso a spiare, ma il suo keylogger genera del traffico di rete e ciò aumenta la probabilità che possa essere scoperto.
Come dicevo all'inizio, i keyloggers odierni hanno la possibilità di configurare numerosissime opzioni. Ho già ricordato la possibilità di inviare il log via rete. Altre possibili opzioni che l'attaccante può selezionare sono le seguenti

- Criptare il file di log, specificando una password che lo renda l'unico in grado di decifrarlo;
- Selezionare nome e percorso del file di log;
- Pianificare l'attività di monitoraggio del sistema. Ad esempio può selezionare i giorni in cui il keylogger deve avviarsi e specificare anche le ore di funzionamento. In questo modo se l'attaccante sapesse in quali ore la macchina bersaglio è maggiormente soggetta a carico di lavoro potrebbe decidere di avviare il suo keylogger in un altro momento, oppure proprio in quel momento visto che un' ulteriore occupazione delle risorse desterebbe minori sospetti;
- Decidere quali tasti dover registrare nel log: per esempio l'attaccante potrebbe non essere interessato alla pressione di tasti come CTRL oppure CANC. Oppure potrebbe essere interessato solo alla pressione di tasti numerici. Questa opzione è interessante nel caso in cui l'attaccante sappia esattamente cosa vuole sapere ed evita che il file di log si riempia di informazioni a lui non utili.

- Stabilire data e ora dell'autodistruzione del programma: l'attaccante potrebbe prevedere che nel giro di due mesi è in grado di catturare il numero di carta di credito della sua vittima e quindi, trascorso questo tempo, cancella le prove della sua intrusione facendo sì che il programma si cancelli.

Ricordiamo che molti keylogger registrano nel log anche le applicazioni che l'utente apre e offre anche vari dettagli su di esse. Ad esempio se l'utente sta ascoltando un file mp3 il keylogger è in grado di stabilire quale mp3 sta ascoltando.

Sopra ho parlato dei keyloggers hardware. Mettendoci dalla parte dell'attaccante, cosa è meglio usare? Un dispositivo hardware o un software? Potendo scegliere per l'attaccante risulta più conveniente un dispositivo hardware. Questo per una serie di ragioni. Innanzitutto l'hardware passa molto inosservato. Un sottile cavo come quello presentato sopra difficilmente sarà notato dall'utente della macchina. Quanti di noi, infatti, ogni volta che si siedono davanti al PC, si mettono a controllare l'eventuale presenza di nuovi cavi? Si tenga conto che inoltre pochi sanno che esistono dispositivi di questo genere e quindi non penserebbero mai di subire attacchi in questo modo. Ricordiamo che un attaccante sufficientemente esperto potrebbe essere in grado di modificare la tastiera di un PC in modo da nascondere al suo interno un keylogger. In questo caso l'utente non riuscirà mai a sospettare della sua presenza (a meno che lui stesso non sia molto esperto e comunque molto accorto!). A ciò si aggiunga il fatto che nessun software è in grado di rilevare la presenza di tali dispositivi e nessun software è in grado di disabilitarli. L'installazione di tali dispositivi è inoltre molto semplice, e l'attaccante non deve essere per forza in possesso di un account sulla macchina da attaccare, in quanto il loro funzionamento non necessita l'installazione di drivers. Per ultimo si noti che non c'è nemmeno il problema delle tracce lasciate da un eventuale file di log, in quanto i tasti digitati vengono memorizzati in una memoria interna. Non ci sono però solo dei vantaggi nell'uso di dispositivi hardware. Prima di

tutto per attuare un attacco di questo tipo l'attaccante deve potere avere accesso fisico alla macchina, altrimenti deve per forza ricorrere ad un attacco via software. Inoltre un attacco via software consente di avere più probabilità di rimanere nell'anonimato. Se, infatti, l'intrusione dovesse essere scoperta, è sicuramente non facile risalire al suo autore, mentre nel caso della scoperta della presenza di nuovi dispositivi, i sospetti si restringerebbero a chi ha accesso alla macchina, e l'attaccante potrebbe essere identificato facilmente tendendogli una trappola. Senza contare che l'attaccante può essere colto in flagrante nell'installazione dei dispositivi. Come detto poc'anzi, un keylogger software fa anche di più, come memorizzare anche le applicazioni che l'utente usa. Via hardware questo non è possibile. Infine c'è anche da considerare l'aspetto economico, per quanto non sia una discriminante principale. I keyloggers hardware costano di più, di solito sui 200-300 euro, mentre i software costano sui 24 euro. Quindi la differenza non è certo eccessiva.
Mettiamoci ora dal punto di vista di chi vuole proteggersi da tali attacchi. Per evitare attacchi hardware l'unica soluzione è proteggere fisicamente le macchine, chiudendo a chiave le stanze in cui si trovano le macchine e controllando l'eventuale presenza di nuovi cavi. Inoltre tenere traccia di tutti coloro che vengono a contatto con le macchine, in modo che sia più semplice risalire all'autore di una intrusione. Per evitare attacchi via software bisogna non installare programmi di cui sia dubbia la provenienza, non lasciare l'accesso alle macchine a chiunque in modo che possa liberamente installare dei keyloggers, e proteggersi da virus e Trojan, che, come detto sopra, sono possibili vettori di keyloggers. Ciò che rende un keylogger uno strumento molto amato dagli hackers è il fatto che una volta installato difficilmente può essere individuato. Se il keylogger è stato installato da un virus o da un Trojan, l'antivirus può fare qualcosa solo dopo che tale virus è stato individuato e ben documentato. In questo caso provvederà a rimuovere tutte le componenti installate all'insaputa dell'utente, compresi eventuali keyloggers. Altrimenti se è stato installato manualmente dall'attaccante, l'antivirus non può fare nulla, dal momento che un keylogger non è un virus. A questo punto a dire il vero è anche difficile potersi accorgere della presenza del keylogger. Come già detto il keylogger non lascia tracce di sé, non compare tra i processi running e il file di log di solito è ben nascosto nel file system. Dal momento che i keylogger solitamente vanno in esecuzione all'avvio del sistema operativo, potrebbe destare sospetti un rallentamento della machina proprio in questa fase, anche se, essendo i moderni calcolatori ormai molto veloci, è difficile fare caso a ciò. Un altro modo è sperare che il keylogger tradisca la sua presenza generando del traffico di rete per inviare via mail il log. Quindi è sempre buona regola tener sotto stretto controlla il traffico via rete per notare se avviene qualcosa di sospetto. Infine sul mercato sono disponibili numerosi prodotti anti-keylogging, purtroppo sempre a pagamento.

Come conclusione presentiamo un esempio di ciò che si può trovare in rete. Il prodotto in questione è Key2Ghost attualmente arrivato alla versione 4. Tale prodotto è pensato "per la famiglia", nel senso che non è prevista l'opzione di invio del file di log via rete. E' possibile scaricare una versione di prova (www.code-it.com), la quale

non ha nessuna restrizione di tempo, ma non è possibile in nessun modo selezionare le opzioni dell'applicazione, Inoltre ogni tre minuti avverte l'utente della sua presenza. La registrazione costa 24 $.
L'applicazione non richiede alcuna installazione: consta solo di un file eseguibile, ed una volta che viene eseguito rimane nascosto all'utente perché non pone alcuna icona nel menu Start, non è visualizzato tra i processi attivi e non mette entries nel pannello Installazione Applicazioni. L'unica cosa che genera è un file "keyboard.uzy", che non viene visualizzato nel caso che l'utente abbia impostato le opzioni di visualizzazione dei files in modo che non siano visibili i files di sistema, e il file di log, che viene memorizzato secondo il path deciso dall'utente. Tale file registra, oltre ai tasti premuti, anche le applicazioni che l'utente manda in esecuzione.
Un esempio di file di log prodotto dall'applicazione è il seguente:

*//Viene registrata data e ora dell'attivazione del programma. In questo caso la sua attivazione coincide con l'avvio del sistema operativo*
*Key2Log Activated ===> 3/15/02 10:16:47 PM*

*//L'utente manda in esecuzione word e scrive alcune parole*
*Active Window ===> 3/15/02 10:19:38 PM>>Untitled - Word*

*This is a small test in MS Word to capture a few key strokes*

*//L'utente ora manda in esecuzione notepad e digita dell'altro testo*
*Active Window ===> 3/15/02 10:22:38 PM>>Untitled - Notepad*

*this is test number 1 to create a test output log file to display on the product web page.*
*I am now going to reboot the system and give it test 2 now...*

*//La macchina viene riavviata, quindi il keylogger si disattiva….*
*Key2Log Deactivated ===> 3/15/02 10:28:44 PM*

*//.....e al riavvio si riattiva*
*Key2Log Activated ===> 3/15/02 10:31:09 PM*