STORIA DEI KEYLOGGER

Negli anni '70, delle spie installarono i primi modelli di keylogger nell'ambasciata degli Stati Uniti e al consolato di Mosca e San Pietroburgo all'interno di macchine per scrivere modello *Selectric II* e *Selectric III*.

Una prima versione di keylogger in codice è stata scritta da Perry Kivolowitz e pubblicata sui newsgroup *Usenet* il 17 novembre 1983.

Le ambasciate sovietiche usavano macchine per scrivere manuali, al posto di quelle elettriche, per le informazioni classificate, in quanto apparentemente immuni agli attacchi keylogger. Al 2013, i servizi speciali russi utilizzavano ancora macchine da scrivere manuali.

Nel 2000, l'FBI attirò due sospetti criminali informatici negli USA con un elaborato stratagemma, riuscendo a catturare i loro username e password con un keylogger installato segretamente su una macchina che essi utilizzavano per accedere ai loro computer in Russia. L'FBI utilizzò queste credenziali per violare i computer dei sospettati e ottenere le prove per perseguirli.

Nel 2011 sono stati trovati alcuni keylogger USB sul retro dei pc di due biblioteche britanniche della contea del Cheshire (Inghilterra).

Nell'ottobre del 2014 alcuni tecnici dell'Università di Birmingham, mentre eseguivano delle procedure di aggiornamento di un computer in un auditorium, hanno scoperto che uno studente aveva utilizzato un keylogger per rubare le password degli amministratori. Le indagini hanno portato a rintracciare il colpevole, che ne aveva approfittato per alzare i voti di cinque esami. Si ritiene sia il primo caso in cui uno studente inglese viene imprigionato per una truffa di questo genere.

COME DIFENDERSI DAI KEYLOGGER

Il modo migliore per prevenire e curare le infezioni da keylogger è seguire alcuni semplici consigli di sicurezza:

- Installare un buon antivirus e mantenerlo aggiornato. I software di cybersicurezza completi sono in grado di riconoscere la maggior parte delle minacce informatiche, tra cui anche i keylogger.
- Utilizzare l'autenticazione a due fattori e i token di sicurezza per gli account più importanti. Se anche si dovesse essere vittima di un keylogger, l'hacker non potrà accedere ai propri account perché le credenziali di accesso non saranno sufficienti. L'efficacia dei sistemi di sicurezza dipende dal numero di livelli di protezione: più se ne ha, più siamo al sicuro.
- Controllare le connessioni in uscita con un monitor di rete (per utenti avanzati). Con uno strumento di questo tipo si può vedere se sul proprio computer sono presenti servizi che funzionano in background e si connettono a Internet per inviare informazioni. Uno di questi potrebbe essere un keylogger.
- Se si riceve una notifica di un tentativo di accesso non identificato, ad esempio da Google, cambiare subito la password. È buona norma utilizzare password sicure e modificarle periodicamente (vedere brochure "Password e buone pratiche").
- Fare molta attenzione a link e allegati di email sospette o provenienti da mittenti sconosciuti. I phisher sono sempre in agguato e, senza volere, potrebbe scaricare un keylogger sul proprio computer quando si apre un presunto file Excel o un PDF.

RIFERIMENTI

➢ http://www.c3t.it/projects/awareness/articoli&brochure/keyloggers/

POR FESR 2014-2020 obiettivo Crescita e Occupazione (CreO)

KEYLOGGERS

Scopri cos'è un keylogger, come funziona e come difenderti.

COS'È E COME FUNZIONA UN KEYLOGGER

Il cybercrimine è un mondo vasto e complesso. Quasi tutte le truffe e i metodi di furto "analogici" sono stati reinventati in chiave digitale e applicati con effetti ancora più gravi. Ne sono un esempio i **keylogger, malware che registrano i dati immessi tramite la tastiera** del computer o dello smartphone, proprio come i loro predecessori fisici per sportelli bancomat e terminali POS.

In origine, questo tipo di programma non aveva scopi criminali e serviva per registrare le parole che venivano immesse nel sistema informatico, ad esempio per controlli di sicurezza. Come sempre però, la tecnologia apre le porte a nuove funzioni e il modo in cui le utilizziamo dipende solo da noi. Quindi, non stupisce affatto che gli hacker abbiano creato delle versioni criminali dei keylogger.

I **malware keylogger** si installano nei sistemi informatici e si attivano in background quando l'utente usa la tastiera. Registrano le informazioni e le inviano al proprietario (l'hacker), il cui scopo principale è trovare le **credenziali di accesso di account online**, ad esempio i conti di **e-banking** delle vittime. Alcuni keylogger sono così sofisticati da riuscire ad aggirare il controllo dei firewall (vedere brochure "I firewall" per saperne di più) quando si connettono a Internet per inviare i dati che hanno registrato.

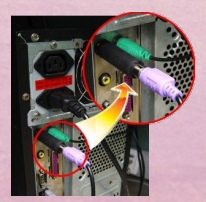
COME SI DIFFONDONO I KEYLOGGER

I keylogger, come la maggior parte dei malware, si diffondono grazie alla **disattenzione degli utenti**: basta un clic su un **link fraudolento** o un **allegato di un'email di phishing** e il programma viene lanciato senza che l'utente se ne renda conto. Poi, dato che si tratta di un software molto piccolo e semplice, questo si attiva in background e non viene notato dalla vittima: il sistema continua a funzionare normalmente, senza rallentamenti o problemi di sorta.

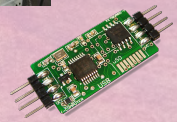
Alcuni keylogger si intrufolano nei computer insieme ad altri programmi pseudolegittimi. Anche in questo caso, la vera causa dell'infezione è l'**ingenuità** dell'utente: se ad esempio scarichi un programma o un file con i **torrent** (piccoli file che contengono informazioni su come scaricare file più grandi utilizzando un particolare protocollo), devi tenere presente che potrebbe essere infetto e contenere un malware.

TIPI DI KEYLOGGER

Hardware keylogger - Dispositivi elettronici che intercettano il segnale dei tasti premuti.



- Hanno l'impiccio di dover essere recuperati dopo l'attività di spionaggio.
- Possono essere piccoli dispositivi che funzionano come connettori hardware che collegano la tastiera al computer e sono progettati per assomigliare a normali connettori di tastiere.
- Possono essere moduli che richiedono di essere installati all'interno della tastiera.



Software keylogger - Programmi che girano in background sul dispositivo vittima.

- Non richiedono l'accesso fisico al dispositivo infettato.
- Registrano ogni sequenza di tasti che l'utente digita, trasferendo periodicamente via web le informazioni a chiunque abbia installato il programma.