

CARPENTIER Julien – CHATELAIN Arnaud

M1 Informatique

MIF30 - Cryptographie



Les keyloggers

Table des matières



1. Définition générale
2. Zones d'insertion de keyloggers
3. Keyloggers matériels
4. Keyloggers logiciels
 1. Présentation des attaques
 2. *Revealer Keylogger*
5. Conclusion

Définition générale



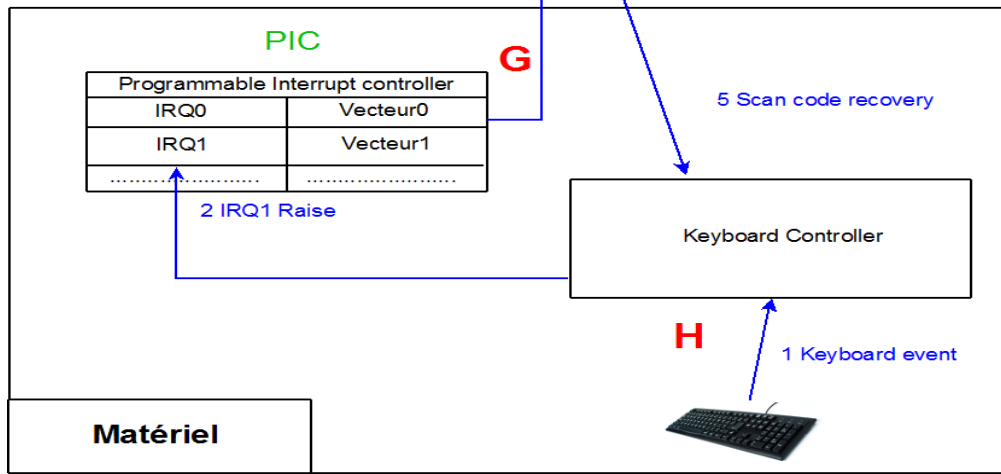
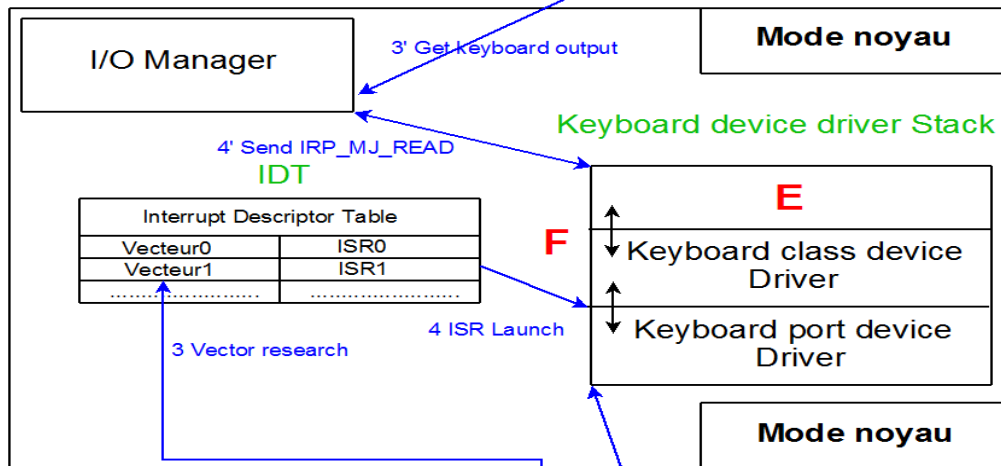
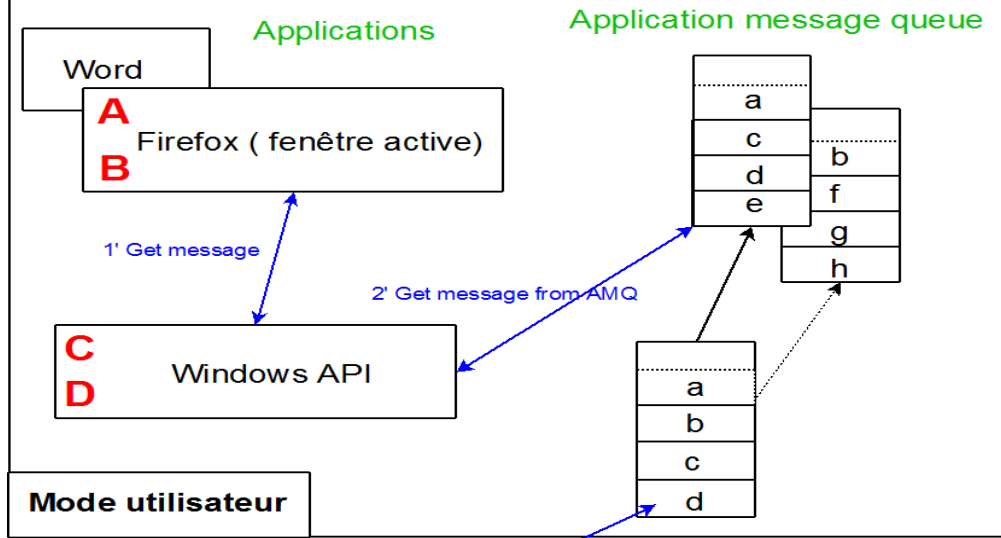
- Les keyloggers permettent la récupération d'informations via le clavier et la souris
- Utilisation frauduleuse récupérant les « login/password » pour l'accès à des données sensibles
- Les keyloggers se présentent sous deux formes : logiciel ou matériel
- Utilisation de manière légale pour l'administration et la surveillance à distance

Zones d'insertion des keyloggers



- Niveau matériel
- Niveau noyau
- Niveau utilisateur

Cheminement d'une saisie clavier sous Windows XP



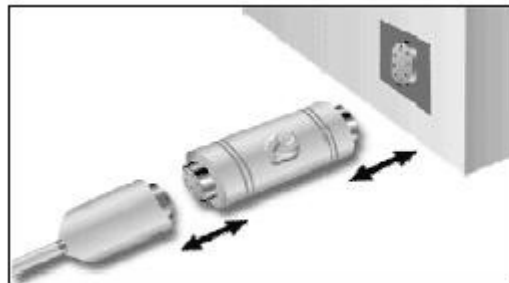
Keyloggers matériels (1)



- Dissimulation d'un module comportant un micro-contrôleur



- Intercalage du Keylogger entre le branchement clavier et la carte mère



Keyloggers matériels (1)



Avantages	Inconvénients
- Détection difficile	- Attaque « physique »
- Aucune installation logiciel	- Keylogger visible (check-up)
- Utilisation simple	- Matériel modulaire (électronique)
- Actif au démarrage (bios)	- Récupération « hors-contexte »
	- Clavier virtuel non géré

Keyloggers logiciels (1)

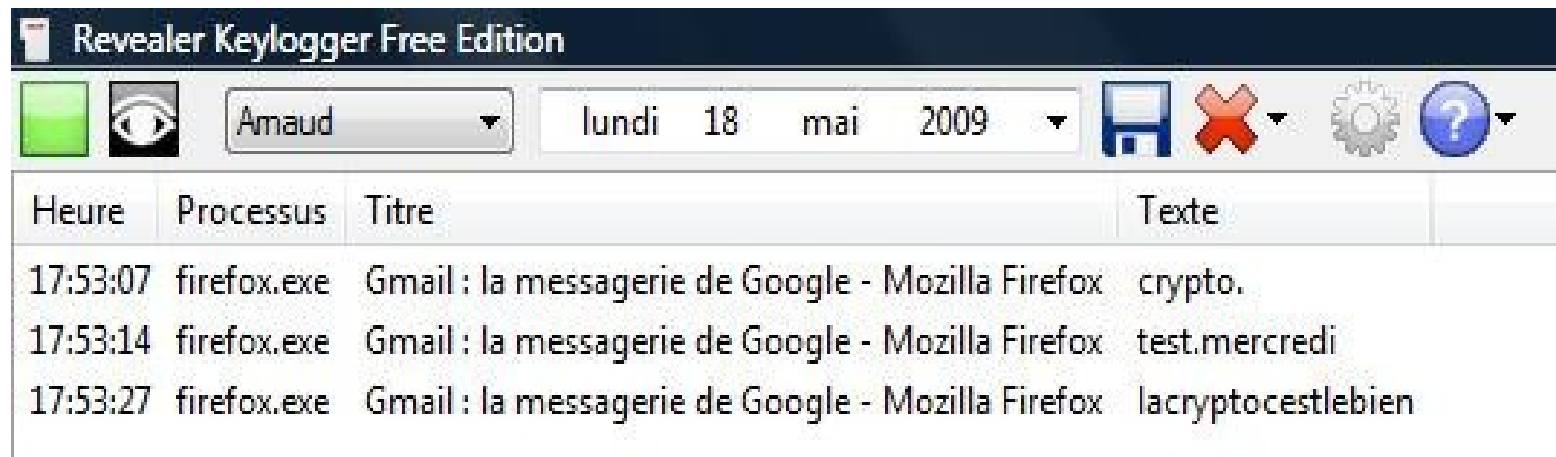


1) Présentation des attaques

- Browser Helper Object
- Requête cyclique
- Le Hooking
 - L'API Hooking
 - SSDT Hooking
 - INLINE Hooking
- Modification des entrées de l'IDT
- Ajout d'un driver périphérique

Keyloggers logiciels (2)

2) Revealer Keylogger



Heure	Processus	Titre	Texte
17:53:07	firefox.exe	Gmail : la messagerie de Google - Mozilla Firefox	crypto.
17:53:14	firefox.exe	Gmail : la messagerie de Google - Mozilla Firefox	test.mercredi
17:53:27	firefox.exe	Gmail : la messagerie de Google - Mozilla Firefox	lacryptocestlebien

Conclusion (1)



- Les keyloggers sont développés en basic ou en C
- Attaques portées sur des système Windows (+ de failles)
- Des solutions de contre-mesure existent (clavier virtuel)...
...mais se font rapidement contourner (flux vidéo, screenshot + keylogger)
- Keylogger logiciel —▶ anti-trojan ou anti-spyware
- Keylogger matériel —▶ inspection matériel régulière

Répartition des différentes attaques « keyloggers logiciels »

