CARPENTIER Julien (10604288)
CHATELAIN Arnaud (10302879)

M1 Informatique

MIF30 : Cryptographie

Les Keyloggers

2008-2009

Table des matières

1. Définition générale [REF02]

Un **keylogger** ou **enregistreur de frappe** peut être considéré comme un logiciel espion (*spyware*) ou un matériel espion dans la mesure où, il a la particularité d'enregistrer les informations frappées au clavier sous certaines conditions, puis de les transmettre via les réseaux ou via des ondes électromagnétiques. Le keylogger intercepte le code d'une touche clavier entre le moment où l'utilisateur effectue l'action et l'exécution de cette action par l'application concernée.

Les enregistreurs de frappes permettent notamment d'enregistrer les codes secrets et mots de passe des sites visités, d'enregistrer les URLs visitées, les courriers électronique consultés ou envoyés, les fichiers ouverts ou encore de créer une vidéo permettant de retracer toute l'activité de l'ordinateur. D'autres fonctions sont également disponible afin de masquer l'activité du keyloggers à l'utilisateur.

Quand l'utilisateur enfonce une touche (ou effectue un clique sur un bouton de la souris), cette action est interprétée par la machine en suivant plusieurs étapes. Le concepteur du keylogger peut donc choisir telle ou telle étape pour intercepter l'action. Grâce à ces fonctions, les keyloggers peuvent être utilisés par des personnes mal intentionnées qui ont pour but de récupérer des informations sensibles comme les mots de passe ou encore les numéros de compte bancaire (utilisés pour les accès bancaire en ligne). Ainsi, l'utilisateur se doit d'être vigilant lorsqu'il utilise un ordinateur « public » en accès libre que ce soit dans une école, un cybercafé, une entreprise, etc.

Les keyloggers se présentent sous deux formes, soit logiciel, soit matériel. Les keyloggers logiciels sont le plus souvent des processus furtifs journalisant une ou plusieurs activités de l'ordinateur (clavier, souris, etc..) dans un fichier le plus souvent crypté. L'activité se fait en fond de tâche à l'insu d'un utilisateur peu vigilant. La seconde forme de keylogger, sont les keyloggers dit « matériels ». Il s'agit d'un dispositif physique installé sur la machine (câble ou dongle) intercalé entre la prise clavier de l'ordinateur et le clavier ou directement inclus dans le périphérique.

Outre l'utilisation illégale et mal intentionnée de cette méthode, on peut également se servir d'un keylogger pour contrôler les touches frappées au clavier, les cliques de souris, les emails lus, etc... d'une machine locale ou distante pour des besoins personnels. Cela permet par exemple de retracer certaines étapes d'une journée de travail. Les keyloggers peuvent aussi être utilisés par des enquêteurs afin de surveiller à distance d'autres ordinateurs, collecter des preuves liées à l'ordinateur ou encore détecter des tentatives d'accès non-autorisées à l'ordinateur et au matériel.

2. Différentes zones d'insertion de keyloggers (Windows)

Les keyloggers permettent d'intercepter les données représentées par les touches de clavier à différents niveaux, suivant le cheminement d'une saisie clavier. Le schéma suivant représente les différentes étapes d'une saisie de clavier et les différentes possibilités d'insertion de keyloggers. Les attaques possibles sont les lettres majuscules en rouge, elle seront décrites un peu plus loin.

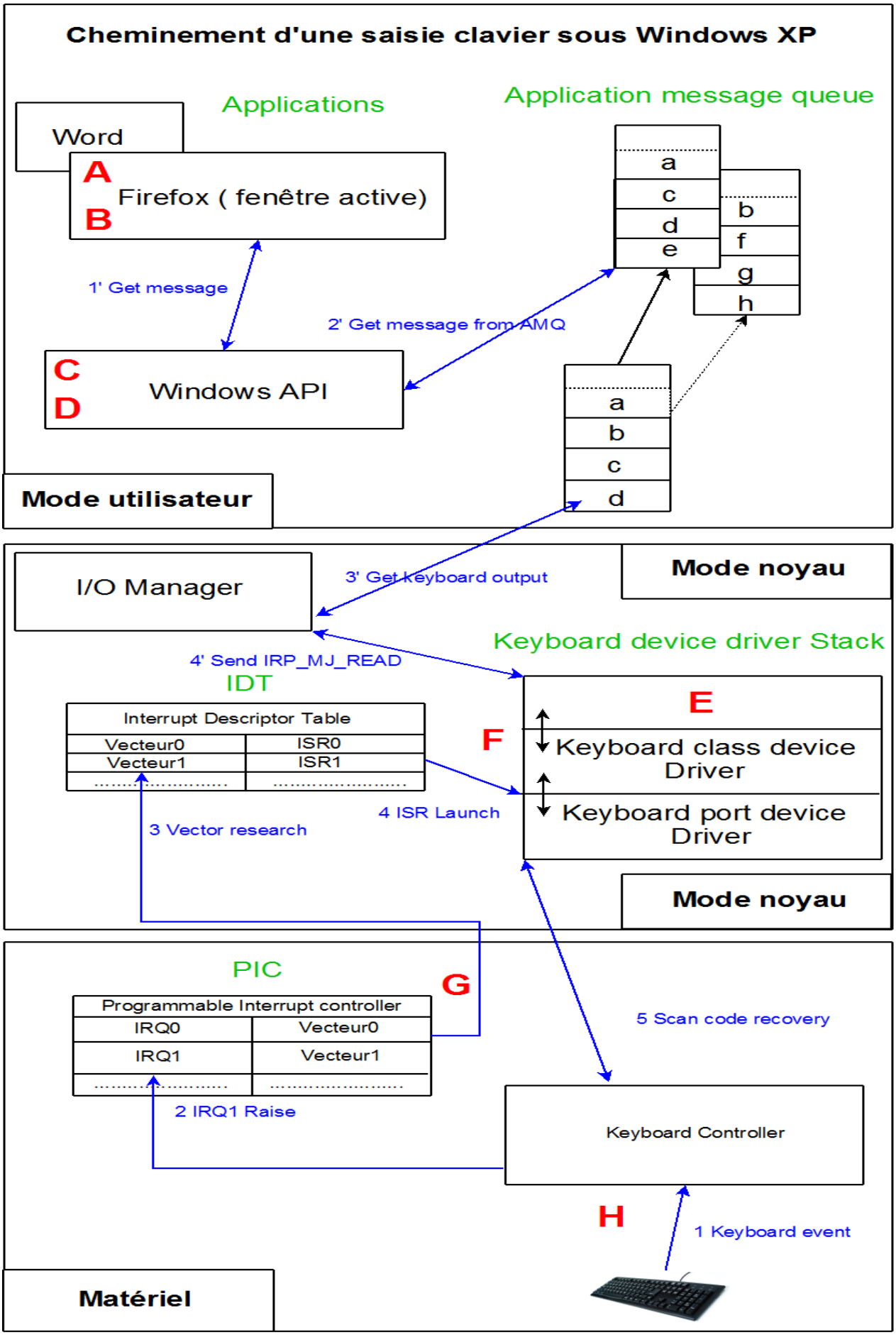

Figure 1 : cheminement d'une saisie clavier

Le cheminement d'une saisie clavier se déroule selon plusieurs étapes et à différents niveaux, voici la description succincte:

Niveau matériel:

1) Lorsque l'utilisateur enfonce, relâche ou maintient une touche du clavier, l'encodeur du clavier envoie le scan code (valeur identifiant la touche sur le modèle du clavier) à la carte mère.
2) Le micro-contrôleur de la carte mère génère une interruption matérielle (IRQ1) pour le traitement de la saisie clavier.
3) Le PIC (*Programmable Interrupt Controller*) permet de maintenir une table de correspondance entre les IRQs et les vecteurs d'interruption.

Niveau Noyau:

4) L'IDT (*Interrupt Descriptor Table*) donne l'adresse de fonction de traitement (*Interrupt Service Routine*) en fonction du vecteur d'interruption.
5) L'ISR enclenche la lecture par le driver du clavier du scan code de la touche présent dans le buffer du microcontrôleur, Le driver convertit ensuite ce scan code en virtual key code correspondant au rôle de la touche appuyée.

Niveau Noyau-Utilisateur:

3') L'I/O Manager transmet ces informations sous la forme d'un message à la System Message Queue puis le message est posté dans l'Application Message Queue du thread destinataire.
1') et 2') Le thread récupère le message puis le transmet à la fonction de l'application traitant les entrées clavier.

Toutes les lettres rouges en majuscule sont les endroits où l'on peut introduire des attaques par keylogger, qui dans la plupart des cas, capturent toutes les frappes clavier effectuées même si un tri selon les applications est possible.

A: Extension standard.
B: Patching de l'application.
C: SetWindowsHookEx().
D: GetAsyncKeyState().(annexe 1)
E: Layered Driver.
F: Major IRP function Table Hook.
G: IDT Hook.
H: Keylogger matériel.

Nous présenterons quelques unes de ces attaques un peu plus loin.

3. Keyloggers matériels (Hardware)

Ce sont les keyloggers les plus bas niveau. Par l'intermédiaire de ce type de keyloggers deux types d'attaques « physique » sont possible :

- Dissimulation d'un module comportant un micro-contrôleur à l'intérieur même du clavier permettant d'intercepter les communications entre le clavier et la carte-mère

Figure 2: Keylogger matériel modulaire

- Le keylogger est intercalé entre le branchement clavier et la carte mère sous la forme d'une clé USB ou d'une extension du port PS/2 (voir figure 3)

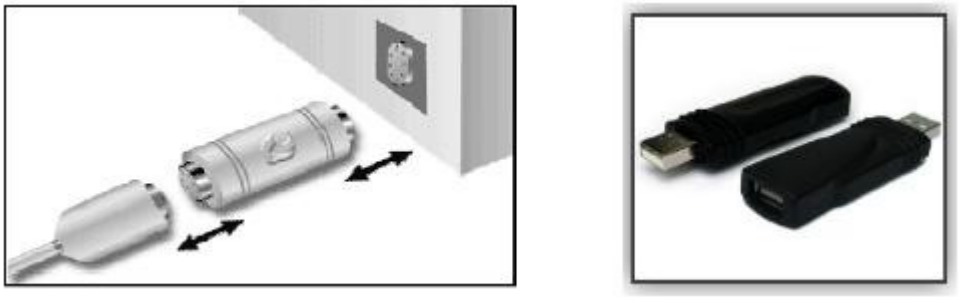

Figure 3 : Keylogger inline

Avantages de l'attaque :

- Difficile à détecter même avec un logiciel (à cause du peu d'énergie utilisé par le keylogger).
- Aucune installation logiciel ni pour le fonctionnement, ni pour la récupération du fichier log.
- Installation simple à la portée de tous.
- Interception de toutes les données transmises par le clavier, et ce dès le démarrage de la machine permettant notamment la récupération du mot de passe du BIOS.

Inconvénient de l'attaque :

- L'installation doit se faire physiquement donc l'utilisateur doit avoir accès à la machine.
- La victime peut détecter le keylogger inline en vérifiant l'installation matériel de son poste.
- L'installation du matériel modulaire (micro-contrôleur à l'intérieur du clavier) prend du temps et nécessite d'avoir un minimum de connaissance en électronique.
- La récupération des données se fait hors-contexte, c'est-a-dire qu'il n'y a aucune relation entre les données récupérées et les applications correspondantes.
- Récupération des données saisies avec un clavier virtuel impossible.

4. Keyloggers logiciels (Software)

4.1. Présentation des attaques les plus répandues

Les keyloggers logiciels, bien que plus aisément détectable par l'utilisateur, possèdent tout de même plus d'avantage que les keyloggers matériel. En effet, un keylogger matériel se contente uniquement d'enregistrer les frappes clavier « hors-contexte » c'est-à-dire sans relation avec l'application ou l'environnement utilisateur concerné. Un keylogger logiciel permettra lui de récupérer non seulement les frappes clavier mais également l'état de la machine cible (et donc l'application correspondante) au moment de cet enregistrement. Les applications les plus ciblées sont les navigateurs web car ils permettent la récupération d'identifiant et de mot de passe (bancaire par exemple) que le pirate pourra ensuite utiliser directement depuis son poste. Il existe plusieurs types d'attaques de type « keylogger logiciel », cependant, certaines sont largement plus utilisées que d'autres (Annexe 2) [REF04] .

Installation d'un Browser Helper Object (BHO) avec Internet Explorer

Il s'agit d'une application tierce partie (de type « plug-in ») qui une fois installée ajoute des fonctionnalités (recherche, anti popup, correction orthographique, etc.) à un navigateur. Cependant certains BHO peuvent être nuisible et n'intègre aucun moyen de les désinstaller. Ainsi, il est tout à fait possible d'intégrer un BHO ayant pour fonctionnalité l'enregistrement de frappe clavier dans le navigateur.

Dans le cas de Firefox il est également possible de rajouter un keylogger grâce au plug-in. Afin qu'il soit difficilement détectable le code de ce keylogger doit contourner les mesures de détection anti-virus et anti-spyware.

Requête cyclique sur toutes les touches clavier et les cliques souris

Il s'agit du type d'attaque le plus basique concernant les keyloggers. Il s'agit tout simplement d'une boucle s'appuyant sur l'API windows.h (sous windows XP) permettant grâce à la fonction GetAsyncKeyState() de connaître l'état d'une touche (*virtual-key code*) à un instant donné. Cette boucle permet donc de récupérer toutes les informations saisies par l'utilisateur.

Voir exemple d'implémentation tiré du magazine MISC [REF01] (annexe 1)

Le Hooking

Le hooking permet de maintenir dans le temps un accès frauduleux à une application sans altérer le noyau du système d'exploitation.

- L'API Hooking : Attaque en mode utilisateur (user-mode)

Les API (*Application Programming Interfaces*) sont des fonctions, procédures ou classes mises à disposition des programmeurs. Les API sont implémentées grâce à des DLL, par exemple sous windows **Win32.dll**, **Kernel32.dll** ou encore **User32.dll** . Cependant, lorsqu'une application veut accéder à une fonction de l'API, elle n'appelle pas directement la DLL concernée, elle utilise l'IAT (*Import Adresse Table*) qui permet de lister les adresses mémoires de toutes les fonctions de chaque DLL utilisée par l'application.

Le principe de l'API Hooking est donc de détourner le lien vers une fonction présente dans l'IAT afin de le faire pointer vers une autre fonction que le pirate aura lui-même définie. Il suffit donc de patcher à la volée l'IAT pour réussir cette attaque. Ainsi, on peut dire que l'API Hooking est une attaque locale à une application car chaque application possède sa propre IAT. Pour prendre le contrôle complet d'une machine il faut donc patcher l'IAT de chaque application active sur la machine. La technique la plus simple pour contaminé une application est de modifier la clé de la base de registre qui liste les DLL automatiquement exécuté lors du lancement de l'application afin d'ajouter la DLL « pirate » .

- SSDT Hooking : attaque en mode noyau (Kernel-mode)

Pour effectuer des opération dites de « bas niveau », une application à besoin d'appeler le noyau système. Le passage du mode « utilisateur » (ou *User-mode*) au mode « noyau » (ou *Kernel-mode*) se fait soit en déclenchant une interruption, soit en utilisant des registres spéciaux du processeur appelé registre MSR. Cependant, quelque soit la méthode utilisée, une fois que le noyau prend la main il utilise une table d'indirection appelée la SSDT (*System Service Descriptor Table*).

De même que pour l'API hooking, il s'agit là d'une modification de l'entrée de la table afin de la faire pointer vers une fonction « pirate », mais contrairement à l'API hooking, ce détournement s'effectuera sur toute les applications s'exécutant sur la plateforme. Pour réaliser une telle attaque, le pirate doit s'infiltrer dans le noyau via une faille dans un service noyau où en installant un driver modifié.

- INLINE Hooking : attaque en mode noyau

Le "inline hooking" est une variante des techniques vues précédemment. Cette fois, plutôt que de modifier une entrée dans une table d'indirection (IAT ou SSDT), cette technique consiste à écraser les premiers octets de la fonction pointée par la table d'indirection.

Pour poser son *hook*, le pirate :

- regarde l'adresse pointée par l'entrée de la table qu'il veut « *hooker* »,
- sauvegarde les premiers octets trouvés à l'adresse pointée,
- écrase ces premiers octets par un code qui détourne l'exécution normale vers une fonction définie ailleurs par le pirate. Cette fonction pirate utilisera bien sûr les octets sauvegardés pour rétablir, si nécessaire, l'exécution normale.

L'intérêt de cette approche est qu'elle est plus difficile à détecter qu'une modification directe sur les tables IAT ou SSDT.

Modification des entrée de l'IDT (Interupt Descriptor Table)

On remplace l'ISR (*Interupt Service Routine*) de traitement des interruptions clavier par une fonction contrôlée par le keyloggers.

Ajout d'un driver périphérique dans la pile des drivers clavier

Lors d'une requête d'entrée/sortie, le gestionnaire des entrée/sortie créer une IRP (I/O Request Packet), dans laquelle il alloue un espace mémoire pour chaque driver de périphérique de la pile. L'IRP est ensuite traité par chacun des drivers de la pile.

Le keylogger est inséré dans la suite de drivers traitant les IRPs concernant le clavier et la souris.

4.2. Exemple avec « Revealer Keylogger »

Voici deux screenshots représentant une connexion à un compte mail avec mot de passe caché puis un screenshot sur l'application « *Revealer Keylogger* » :

Figure 4 : Authentification gmail

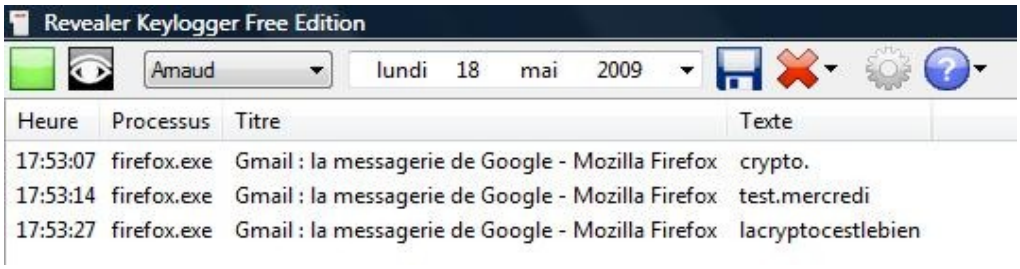

Figure 5 : Log du keylogger

On observe sur ce logiciel que peu importe les informations tapées par l'utilisateur, elle sont récupérées par notre logiciel keylogger avec l'heure, l'application correspondante, l'adresse du navigateur et enfin le texte tapé.

5. Conclusion

Il existe une multitude d'attaques de type « keylogger » plus ou moins facile à implémenter permettant d'espionner les frappes clavier et les mouvements souris. La plupart du temps les keyloggers sont développés en basic ou en langage C. La plupart de ces attaques se font sur Windows car ce système comporte plus de faille que sur Linux ou Mac Os notamment au niveau de la gestion des comptes utilisateurs et administrateurs qui sont souvent confondus.

Certains organismes fortement concernée par ce type d'attaque comme les sites de paiement sécurisé ou encore les banques ont mis en place un système de claviers virtuels permettant aux utilisateurs de pointer les caractères constituant le mot de passe afin de ne pas enregistrer l'événement clic souris associer aux coordonnées sur l'écran. Malheureusement, il suffit d'associer un keylogger à un système de capture d'écran ou de flux vidéo afin de contourner ce système.

En général, il suffit d'un d'un simple contrôle anti-spyware et anti-trojan pour détecter d'éventuels keyloggers logiciels et une inspection régulière du matériel afin de détecter les keyloggers matériels.

6. Bibliographie

[REF01] :
Article de MISC, septembre 2007

[REF02] :
http://fr.wikipedia.org/wiki/Enregistreur_de_frappe

[REF03] :
http://www.certist.com/fra/ressources/Publications_ArticlesBulletins/Environnement_Microsoft/ApiHooking/

[REF04] :
http://www.viruslist.com/fr/analysis?pubid=200676083

7. Annexes

Annexe 1 : Implémentation keylogger « requête cyclique »

```
int APIENTRY WinMain(HINSTANCE hInstance, HINSTANCE hPrevInstance, LPSTR lpCmdLine, int nCmdShow)
{
	 int vKey = 1;

	fdKeylogFile = fopen("GetKeyState.txt", "a+");
	if (fdKeylogFile == NULL) return 0;

	while(TRUE)
	{
		for (int vKey = 1; vKey <= 254; vKey++)
		{
			// Si la touche a été pressée
			if ((GetAsyncKeyState(vKey) & 0x81) != 0)
			{
				 // On enregistre l'évènement dans un fichier
				if (vKey == VK_LBUTTON) logMouseClick(fdKeylogFile);

				else if (vKey >= 65 && vKey <= 90) // Key [A-Z]
					logCharPress(vKey, fdKeylogFile);
				else if (vKey == VK_RETURN) // return
					fwrite("\n", 1, 1, fdKeylogFile);
				else if (vKey == VK_TAB || vKey == VK_SPACE) // tab, space
					fwrite(&vKey, 1, 1, fdKeylogFile);
				else if (vKey >= 48 && vKey <= 57) // Key [0-9]
					logNumPress(vKey, fdKeylogFile);
				else if (vKey == VK_BACK) // backspace
					fwrite("[BACK]", 1, 6, fdKeylogFile);
			}
		}
		fflush(fdKeylogFile);
		Sleep(1);
	}
}
```

Annexe 2 : Répartition des différents types d'attaque « keylogger logiciel»

Remarque : « Piège » correspond ici aux différentes techniques de Hooking.

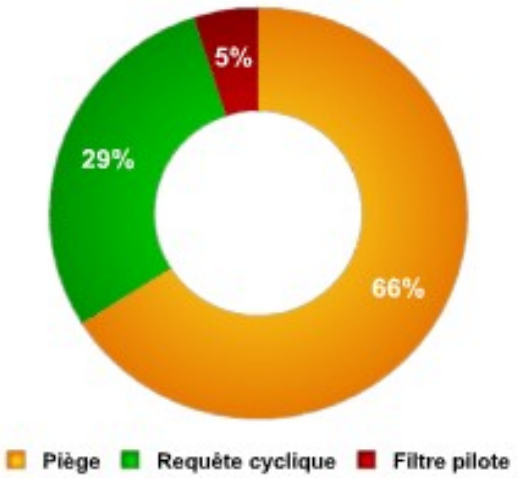

Figure 6 : Keylogger inline