

Convention Sécurité - Juin 2005

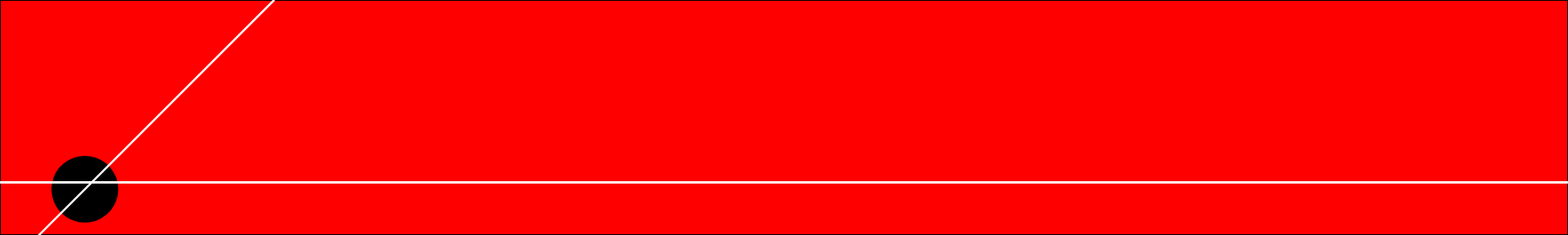
Spywares

David Kopp – Directeur TrendLabs Europe

david_kopp@trendmicro.fr



- I. Introduction de la problématique Spyware**
- II. Grayware (Spyware)**
- III. Questions**



QuickTime™ and a
Microsoft Video 1 decompressor
are needed to see this picture.

Où peut-on trouver des spywares?

The screenshot illustrates a spyware infection on a Windows XP desktop. The primary window is Microsoft Internet Explorer, which is displaying the LYRICS Download.com website. A prominent 'Warning' dialog box is shown, indicating that the user is being redirected to an advertisement for 'WebSecureAlert'. The website itself features a search bar, a list of artists, and a 'WHY REGISTER?' section. The taskbar at the bottom shows the Start button and several open applications, including the LYRICS Download.com browser window.

Warning
Use protect or Download WebSecureAlert.
(advertisement)

WHY REGISTER? (for free)

- No ads for registered members
- Download Lyrics Archiver will feature than 500,000 lyrics
- Help the community to build this archive
- Talk about music and general topics with other members
- More and more things (free lottery, free ad, posters and more weekly for registered members)

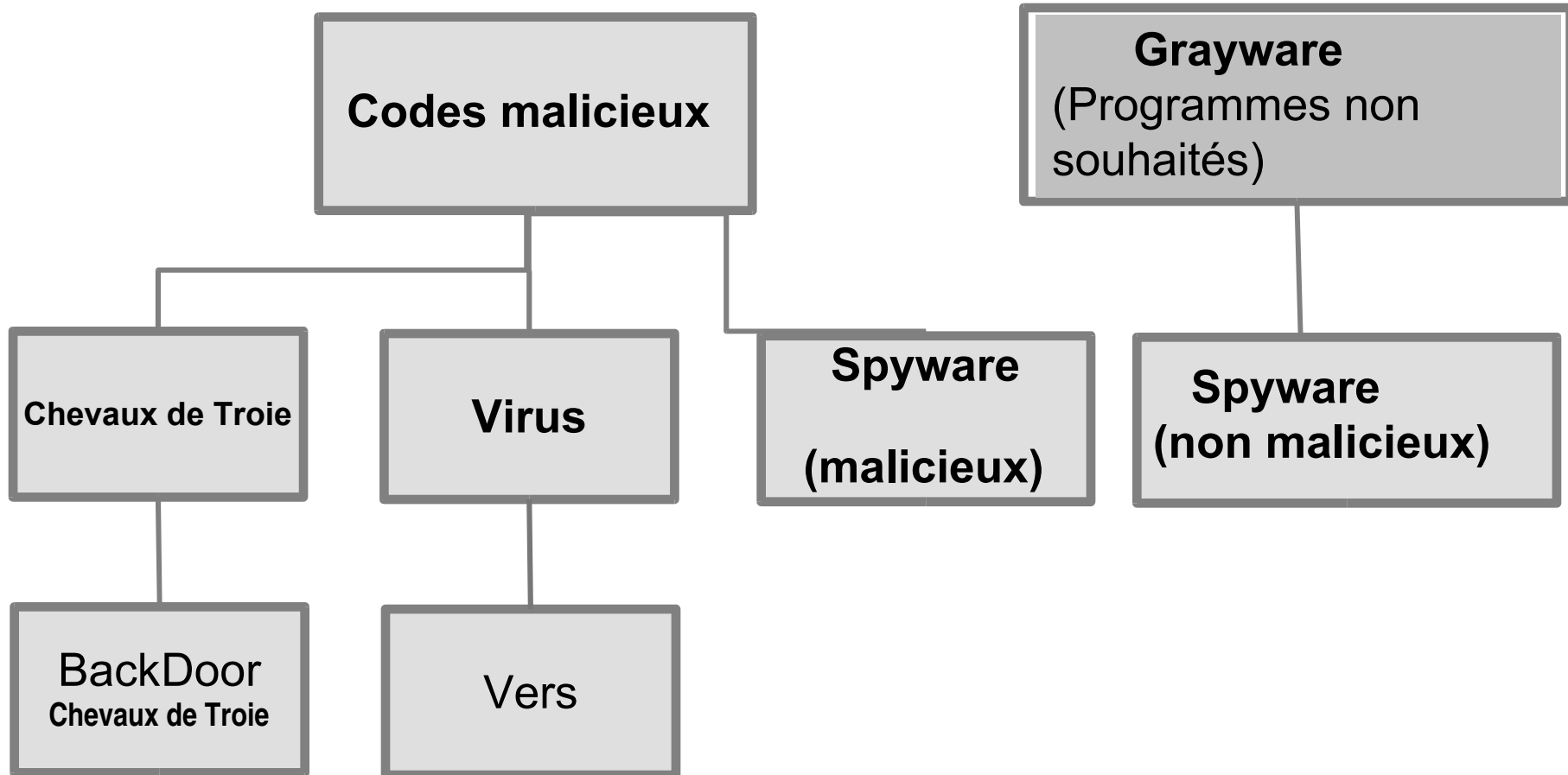
REGISTER HERE TODAY!

Artist	Album	Count
Phish	Phish	1
U2	U2	2
Enigma	Enigma	3
3030	3030	4
Avril Lavigne	Avril Lavigne	5
OMARION	OMARION	6
Maroon 5	Maroon 5	7
Phish	Phish	8
U2	U2	9
Enigma	Enigma	10
3030	3030	11
Avril Lavigne	Avril Lavigne	12
OMARION	OMARION	13
Maroon 5	Maroon 5	14

QuickTime™ and a
Microsoft Video 1 decompressor
are needed to see this picture.

- I. Introduction de la problématique Spyware
- II. Grayware (Spyware)**
- III. Questions

Taxonomie: Les différentes menaces



Grayware

Terme utilisé dans l'industrie pour désigner largement les spywares et autres (le plus souvent légitimes) programmes éventuellement non désirés comme:

- Adware
- Dialers,
- Joke programs,
- Remote Access Programs (RAPs)
- Hacking tools,
- Spyware
- Password Cracking Applications

Grayware

Spyware

Programme récoltant des informations au sujet d'une personne ou d'une organisation pour les envoyer ensuite à des équipes marketing ou tout autre partie intéressée. L'installation, pistage et envoi des informations sont typiquement effectués sans le consentement de l'utilisateur ou sans qu'il en ait connaissance.

La plupart de ces programmes sont des applications légitimes orientées marketing.



Spyware

Event Loggers

Event Loggers

Souvent légitimes, ces programmes enregistrent les événements système pour consultation future ou pour envoi à une partie tierce. Ces événements contiennent souvent les habitudes de l'utilisateur.

Quelles/Quand sont les applications lancées?

Quand le système est-il arrêté/démarré?

Event Loggers

Spyware

ware

Keyloggers

Keyloggers

Peut enregistrer toute frappe clavier et ainsi voler des mots de passe et des informations confidentielles.

Event Loggers

Keyloggers

Spyware

Grayware

Screen Captors

Screen Captors

Ce sont des programmes effectuant des captures d'écran (image ou video) pour ensuite les relayer vers une partie tierce ou alors les stocker sur le système pour une lecture future.

Event Loggers

Keyloggers

Screen Captors

Spyware

Grayware

Adware

Un adware est une application affichant des bannières publicitaires. Un adware contient souvent un spyware pour ainsi savoir quelle est la bonne publicité à afficher en relation avec les habitudes de l'utilisateur.

Event Loggers

Keyloggers

Screen Captors

Adware

Spyware

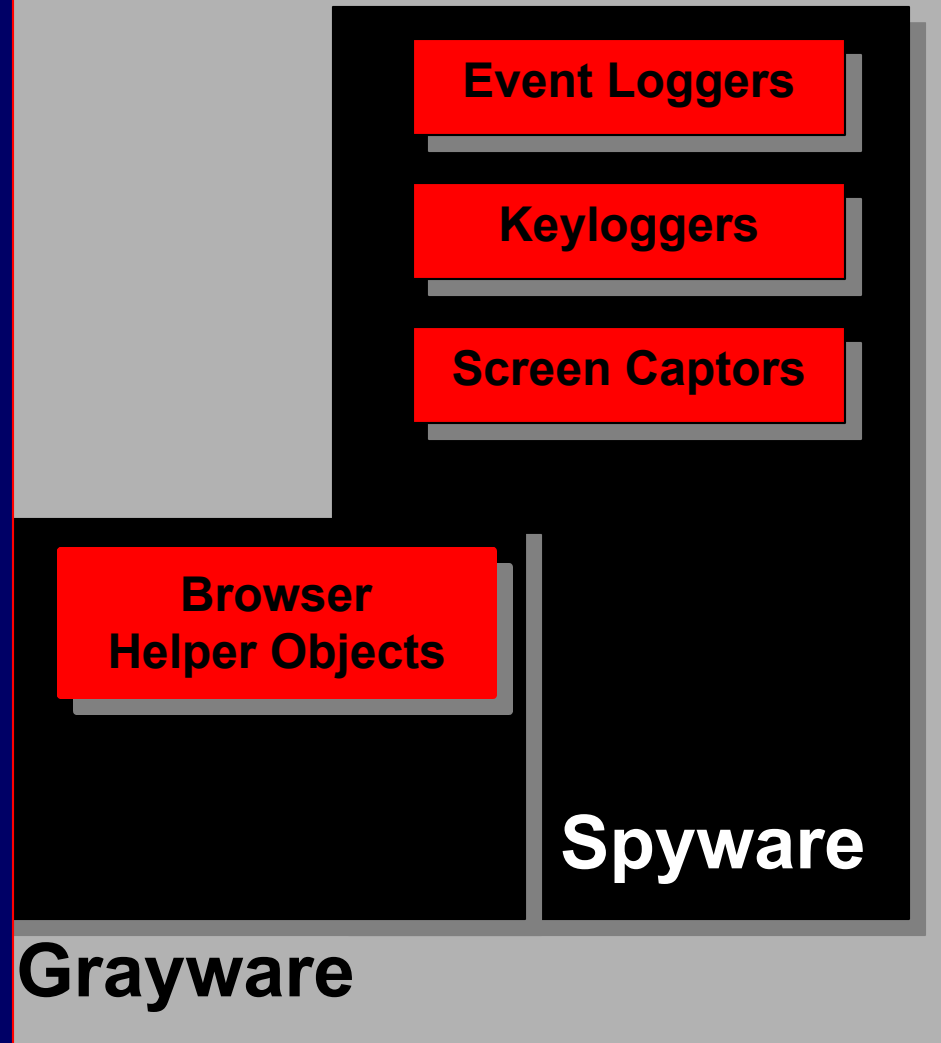
Grayware

Browser Helper Objects

Les **BHOs** sont des applications “compagnons” de Microsoft Internet Explorer.

Ils arrivent normalement sous la forme de toolbars, d'aide à la recherche, et d'applications de surveillance.

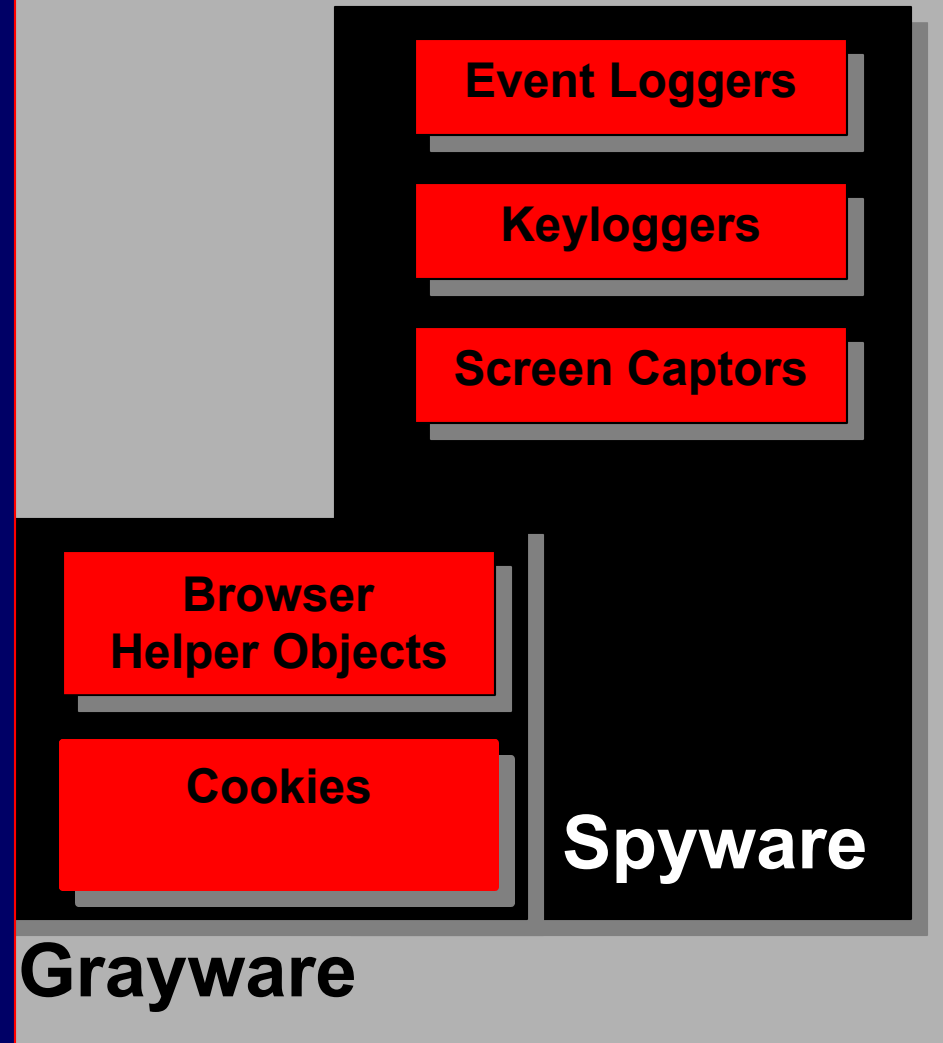
Ainsi les BHOs peuvent surveiller les habitudes de navigation de l'utilisateur et afficher ensuite les “bonnes” publicités ou voler des informations



Tracking Cookies

Tracking cookies

récoltent une large quantité d'information sur les utilisateurs et sont généralement interrogés par plusieurs domaines. Etant typiquement utilisés pour affiner les publicités affichées, ces cookies construisent une image très avancée du profil psychologique et démographique de l'utilisateur.



Hacking Tools

**Hacking
Tools**

Event Loggers

Keyloggers

Hacking Tools

Les Hacking tools sont des programmes qui généralement crackent ou cassent la sécurité d'un système ou d'un réseau. Les administrateurs systèmes ou réseau utilisent des outils similaires – si ce ne sont les mêmes – pour tester la sécurité de leur environnement et identifier de possibles failles.

Adware

COOKIES

Spyware

Grayware

Remote Access Programs

**Hacking
Tools**

Event Loggers

Keyloggers

RAPs

Screen Captors

Remote Access Programs

Aussi connus comme remote access tools (RATs), ces programmes autorisent des personnes à accéder et à contrôler des systèmes distants. Plusieurs de ces programmes sont des programmes légitimes utilisés par tout type d'utilisateurs pour accéder à des fichiers ou données sur des ordinateurs distants.

Dialers

Adware

Dialers:

Les Dialers composent des numéros prédéfinis pour se connecter à certain sites. Plusieurs personnes utilisent ces programmes sans savoir que certains d'entre eux composent des appels longue distance ou se connectent à des sites payant.

Grayware

Joke Programs

Joke Programs

Dialers

Adware

Joke Programs:

Les programmes Joke sont considérés comme relativement sans danger et sont souvent cause de désagrément ou d'amusement pour les utilisateurs. Ils n'infectent pas de fichier, ne causent pas de dommage et ne se propagent pas. Plusieurs d'entre eux tentent de causer un état de panique chez l'utilisateur.

Grayware

Others

Joke Programs

Dialers

Adware

Cookies

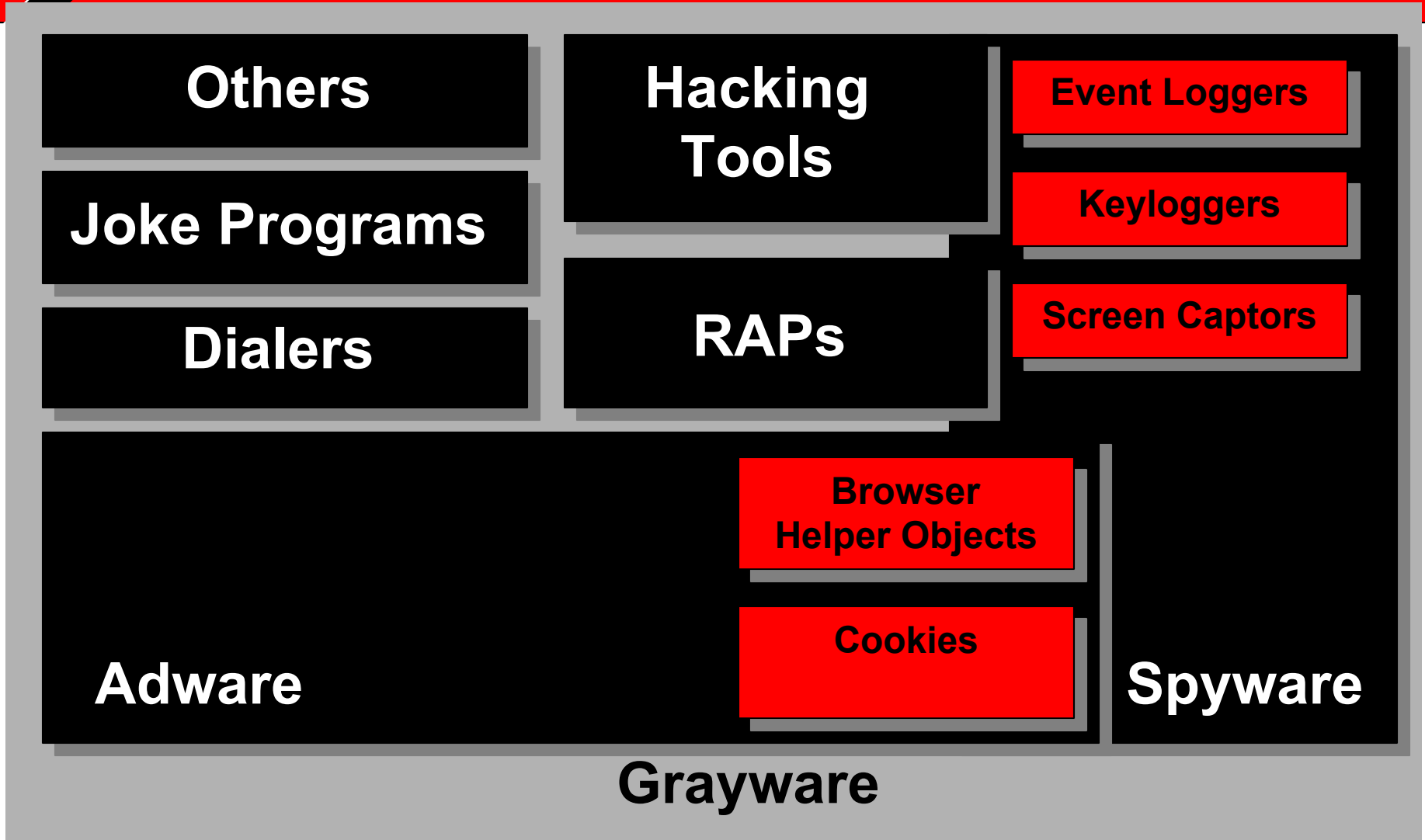
Spyware

Grayware

Others:

Tout autre programme ne trouvant pas sa place dans les sous-familles décrites auparavant.

Vue d'ensemble: Grayware



Exemples de Spyware/Grayware

- GAIN / Gator
- Gator E-Wallet
- Cydoor
- BonziBuddy
- MySearch Toolbar
- DownloadWare
- BrowserAid
- Dogpile Toolbar



Image Sources...

GAIN Logo – The Gator Corporation – <http://www.gator.com>

BonziBuddy Logo – Bonzi.com -
<http://images.bonzi.com/images/gorillatalk.gif>

DownloadWare Logo – DownloadWare - <http://www.downloadware.net>

- I. Introduction to the Spyware Problem**
- II. Grayware (aka Spyware)**
- III. Questions**

David Kopp (david_kopp@trendmicro.fr)

QuickTime™ and a
Microsoft Video 1 decompressor
are needed to see this picture.