

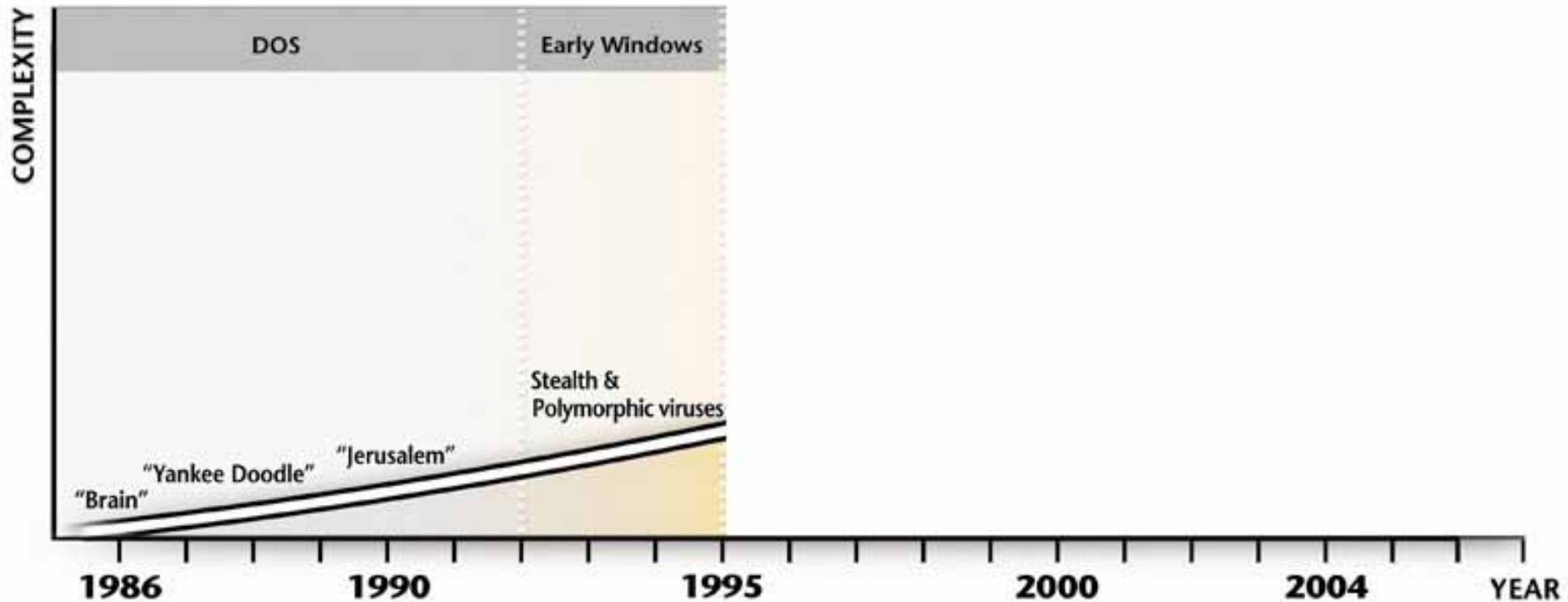
## Les produits FINJAN aujourd'hui ?

---

Lionel Monchecourt

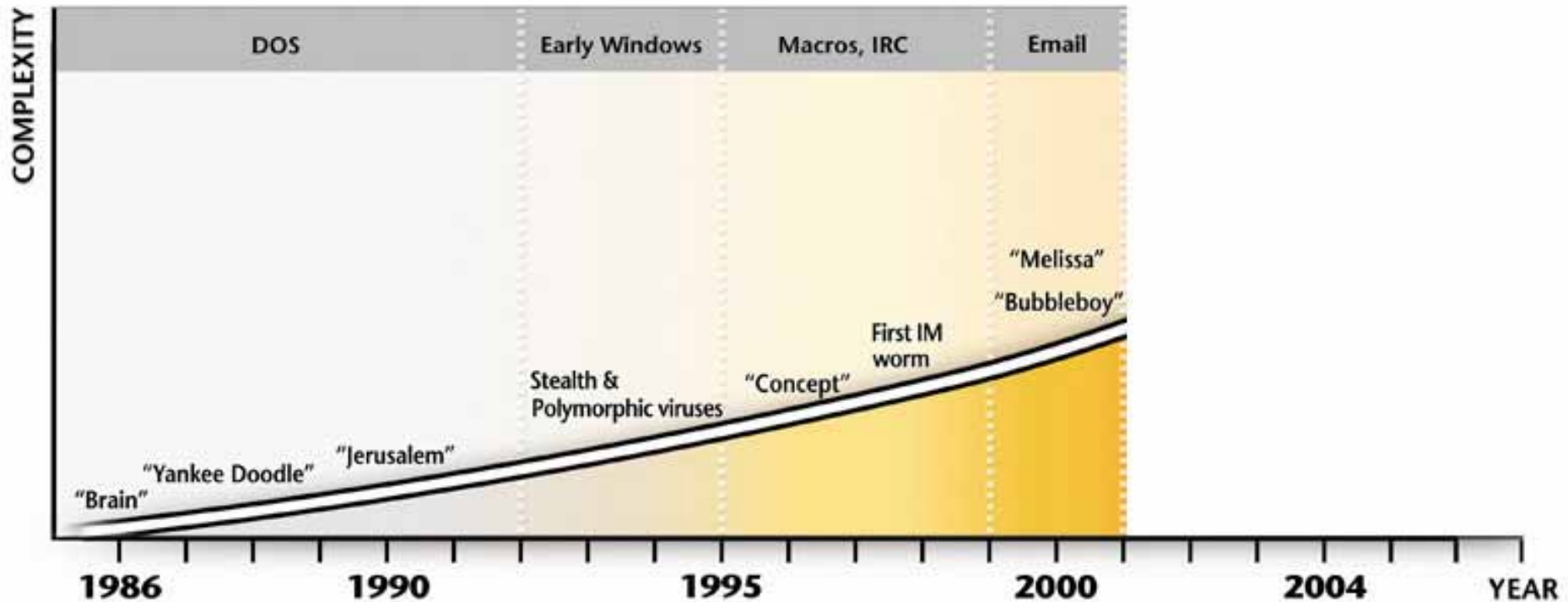
- La menace
  - Historiquement, les auteurs de virus recherchaient une propagation rapide et importante de leur virus afin d'obtenir une NOTORIETE.
    - L'avantage pour les éditeurs d'anti-virus : Isoler rapidement le virus, Trouver rapidement la parade.
  - Aujourd'hui, le but recherché est LUCRATIF.
    - Code personnalisé avec un but bien précis plus difficile à détecter
      - Les buts recherchés
        - » Vol d'informations, espionnage
        - » Destruction d'informations
        - » Mise hors service partielle ou totale du système d'information

# Evolution – à l'époque "déconnectée"



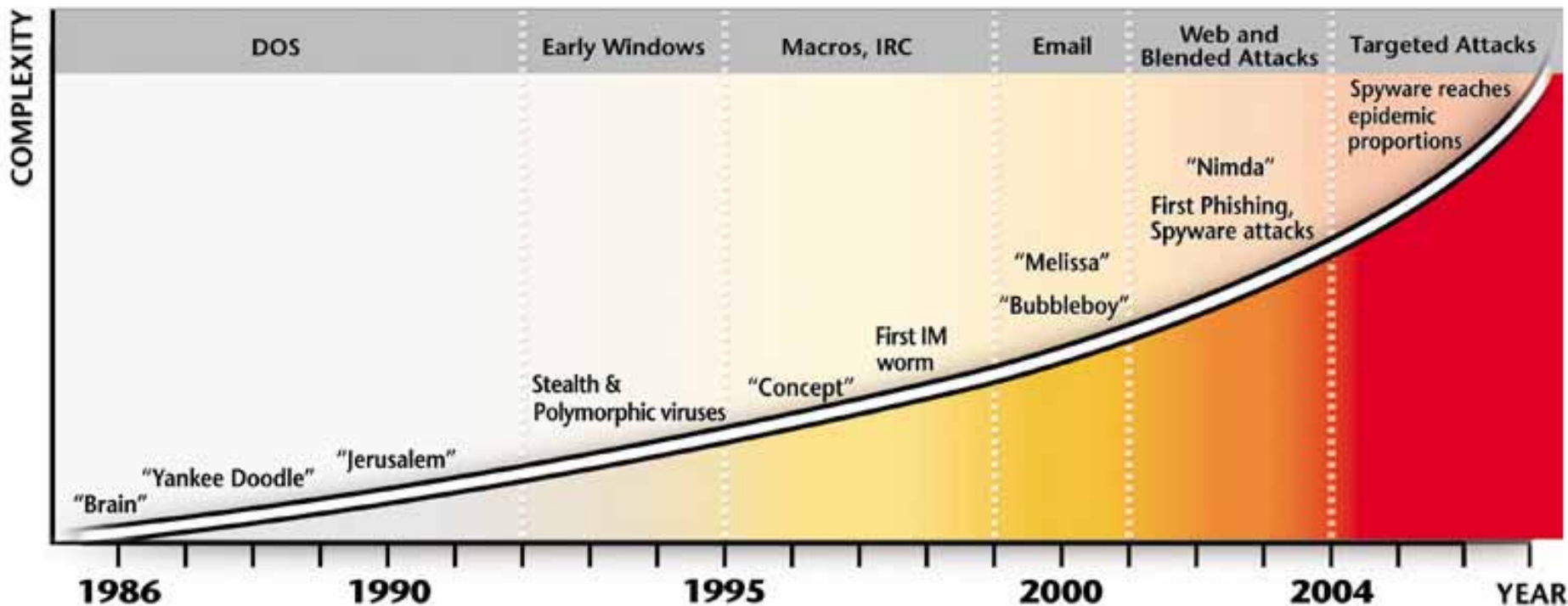
- **Developers:** Geeks
- **Propagation:** Manuelle (push)
- **But:** Notoriété
- **Impacte:** Productivité

# Evolution – Début des connexions



- **Developers:** Geeks
- **But :** Notoriété
- **Propagation:** Electronique (push/pull)
- **Impacte:** Productivité

# Evolution – Connected World



- **Developers:** Criminels
- **But:** \$\$\$\$
- **Propagation:** Electronique (pull)
- **Impacte:** Infos, Propriété intellectuelle

inet-lux | - Microsoft Internet Explorer provided by Finjan

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Refresh Print Mail News RSS Feeds

Address <http://inet-lux.com/index.php?go=Page&id=3> Go Links Cu

Google Search 7 blocked Check AutoLink AutoFill Options

| "Не пытайся избежать своих врагов, а просто контролируй их. Знай где они, что думают и кому верят". |

[=INET-LUX.COM=]

Здравствуйте, Гость | Авторизация | Регистрация

Навигация

- На главную
- О нас
- Новости
- Наши продукты
- Вопрос-ответ
- Оставить отзыв
- Мой офис
- Пресс-центр
- Контакты

Авторизация

Логин:

Пароль:

Запомнить меня

Войти...

[Регистрация](#)  
[Напомнить пароль](#)

Ваше мнение

сколько вы готовы платить за эксплойт?  
100-300\$

Мульти-компонентный эксплойт **Web-Attacker IE0604** (Март 2006г.)


Уважаемые друзья! Мы рады предложить Вам мультикомпонентный эксплойт **Web-Attacker IE0604**, реализующий уязвимости в популярных Интернет-браузерах Internet Explorer и Mozilla Firefox. При помощи данного эксплойта Вы можете устанавливать любые исполняемые программы на локальных дисках посетителей Ваших сайтов. В основе работы эксплойта **Web-Attacker IE0604** лежат семь обнаруженных ранее уязвимостей в Интернет-браузерах:

**Назначение эксплойта:** скрытая загрузка EXE-программы с удаленного ресурса с последующим запуском этой программы на локальном диске посетителя.

**В основе работы эксплойта лежат 7 уязвимостей:**

1. Last Stage of Delirium Research Group, "Java and Java Virtual Machine Security Vulnerabilities and their Exploitation Techniques", <http://lsd-pl.net/>. По классификации Microsoft - **MS03-11**. Цель: машины с Windows 98-XP, браузером Internet Explorer, с установленной Microsoft Virtual Machine версии 5.0.3805.0 или младше.
2. Roozbeh Afrasiabi, "IE ms-its: and mk:@MSITStore: vulnerability", Insecure.org mail archive <http://www.insecure.org/>, Mar 27 2004 По классификации Microsoft - **MS04-012** (Microsoft - Windows 98-XP, браузером Internet Explorer, с установленной Microsoft Virtual Machine версии 5.0.3805.0 или младше).

Отзывы клиентов:



"Знакомый купил связку - говорит она просто охуенная. Он все секреты не выдаёт, но мою тачку и тестовую и настоящую пробило как за не\*\*\* делать".

**JagUarc**

[Оставить отзыв](#)

Done Internet



# Toolkit de piratage de Web – Page de commande

## Downloader - RootLauncher v2.5

Downloader предназначен для скрытой загрузки произвольного WIN32 EXE-файла с удаленного ресурса с последующим запуском этого файла на локальном диске.

Продукты - RootLauncher	[ Цена ]	[ Документация ]	
"Professional Edition" [PE]	150\$   обновления: 20\$	готовится	готовится
"Econom Edition" [EE]	100\$   обновления: 15\$	<a href="#">Онлайн</a>	<a href="#">Офлайн</a>
"Light Edition" [LE]	50\$   обновления: 10\$	готовится	готовится

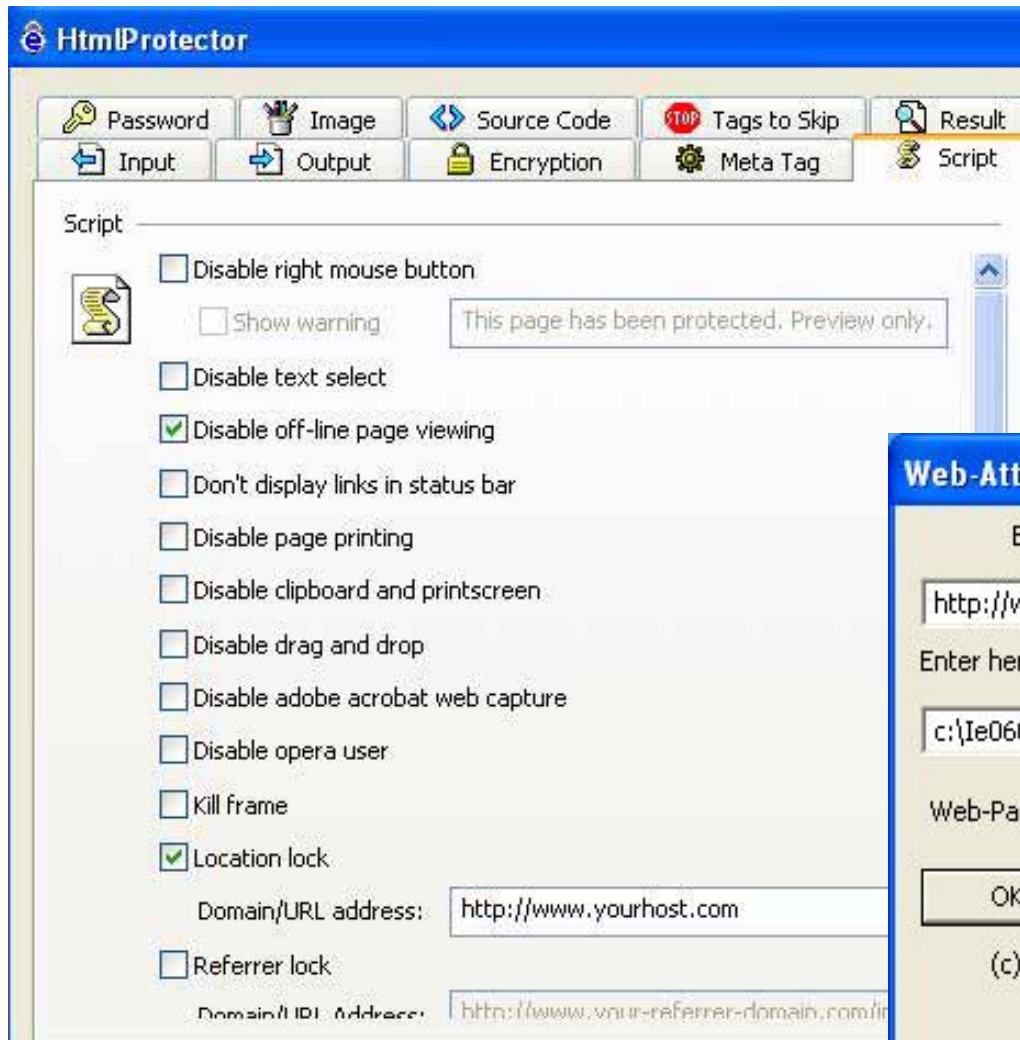
Даунлоадеры - RootLauncher v2.5 не обнаруживаются следующими антивирусами:

[Онлайн - документация](#)

[Офлайн - документация](#)

**Цена : 300\$ (wmz) | Цена обновления: 25\$ (wmz)**

# Toolkit de piratage de Web – Interface Utilisateur





# Toolkit de piratage de Web – Rapports

Exploit penetration statistics - Microsoft Internet Explorer provided by Finjan

Address: http://redcrossonline.cn/cgi-bin/le0604.cgi?password=admin

### Overall statistics

Total hosts	MS03-11	MS04-013	MS05-002	MS05-054	0-Day	MFSA2005-50	MS06-006
2328	80	2	0	8	41	4	0
100.00 %	3.44 %	0.09 %	0.00 %	0.34 %	1.76 %	0.17 %	0.00 %

Total Exploit efficiency is 5.80 %

### Operation Systems statistics

OS name	Hosts	MS03-11	MS04-013	MS05-002	MS05-054	0-Day	MFSA2005-50	MS06-006
Linux	21	0	0	0	0	0	0	0
Mac OS	21	0	0	0	0	0	0	0
PowerPC	4	0	0	0	0	0	0	0
Unknown	53	0	0	0	0	0	0	0
Windows 2000	163	7	0	0	0	0	0	0
Windows 2003	11	0	0	0	0	0	0	0
Windows 98	76	24	2	0	0	0	0	0
Windows ME	36	7	0	0	0	0	0	0

Exploit penetration statistics - Microsoft Internet Explorer provided by Finjan

### Overall statistics

MS04-013	MS05-020	0-Day	MS06-006
3	17	279	0
0.03 %	0.14 %	2.33 %	0.00 %

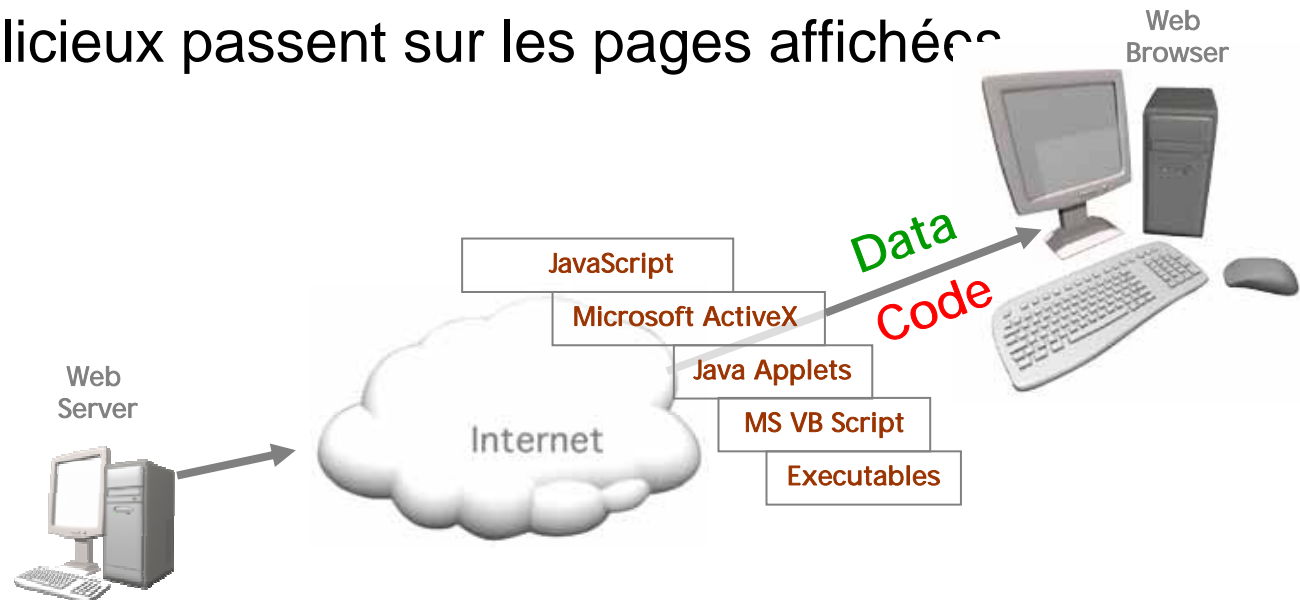
Total Exploit efficiency is 4.38 %

### Operation Systems statistics

OS name	Hosts	MS04-013	MS05-020	0-Day	MS06-006
Linux	73	0	0	0	0
Mac OS	211	0	0	0	0
PowerPC	121	0	0	0	0
Unknown	157	0	0	0	0
Windows 2000	480	21	0	0	0
Windows 2003	17	0	0	0	0
Windows 95	5	1	0	0	0
Windows 98	296	31	0	0	0

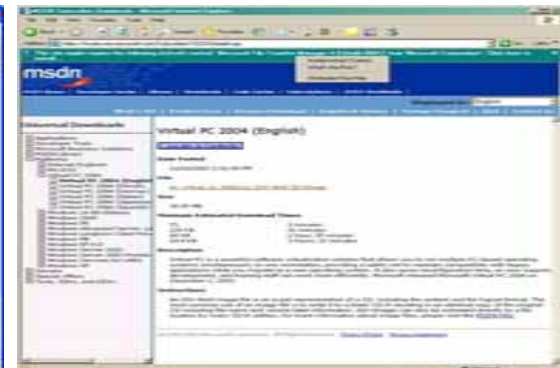
- *Можно ли переименовывать файл `ie0604.htm` ? - Да, этот файл можно размещать на сервере под любым именем, которое будет удовлетворять правилам построения URL-запросов. Предположим, мы разместили на сервере файл `ie0601.htm` под именем `demo.htm`. Тогда посетителей Вашего сайта нужно будет направлять на URL-адрес <http://www.yourhost.com/demo.htm>*
- *При обращении к скрипту `ie0604.cgi` сервер возвращает ошибку 500. Что делать ? - Проверить, разрешено ли конфигурацией данного сервера выполнение CGI-скриптов. Проверить атрибуты у файла `ie0604.cgi`, они должны быть равны 755.*
- *Трафик идет, а в статистике он не отображается. Почему ? - Статистику посещений/срабатываний компонентов эксплойта ведет скрипт `ie0604.cgi`, всю информацию о посетителях он сохраняет в своей же директории, в файле `ie0604.dbf` . Поэтому в первую очередь следует проверить, создан ли файл с таким именем в директории `cgi-bin`. Иногда сервер сконфигурирован так, что CGI-скрипты не могут самостоятельно создавать файлы и в этом случае файл `ie0604.dbf` нужно будет создать предварительно вручную (т.е. просто пустой файл), установив ему атрибуты 666.*

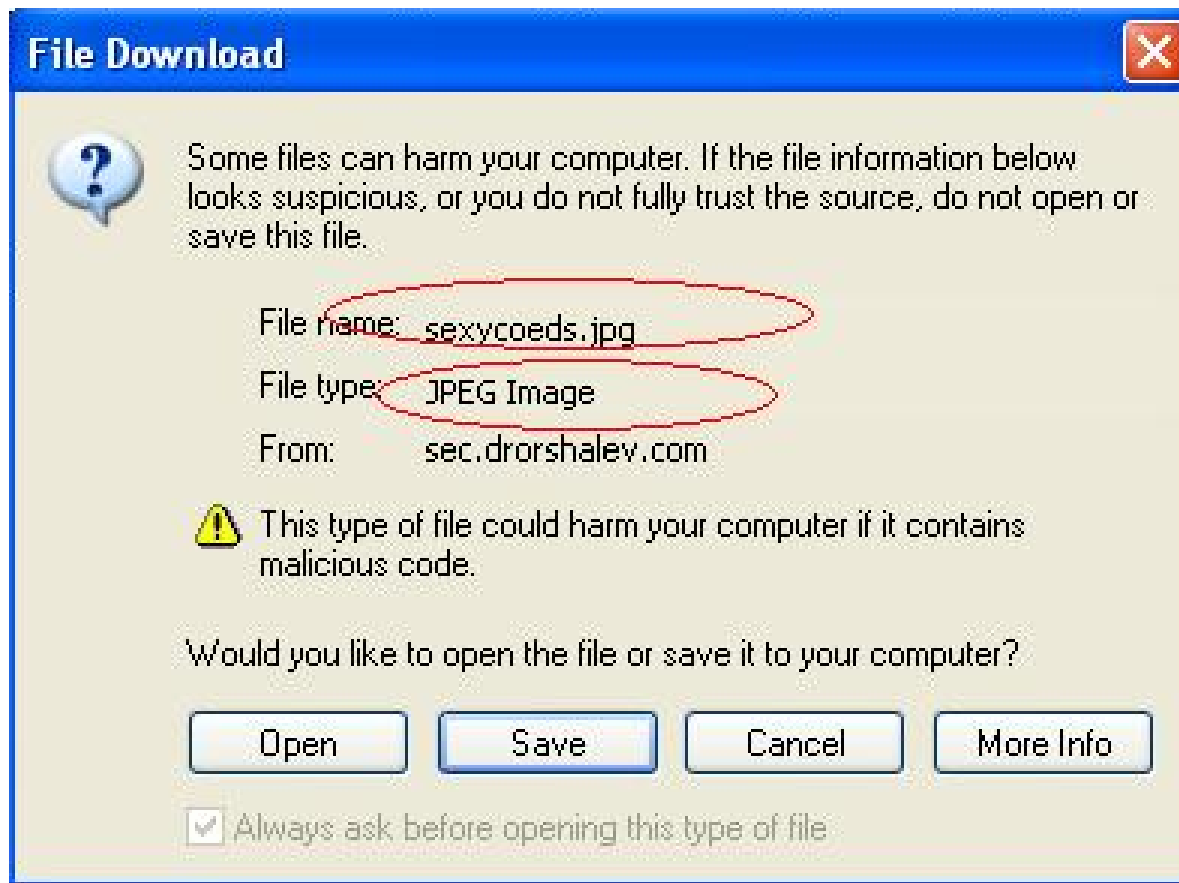
- Aujourd'hui tout le monde sait être méfiant vis-à-vis des emails reçus
- La plupart des utilisateurs n'ont aucune crainte lorsqu'ils naviguent sur le web.
- Les codes malicieux passent sur les pages affichées



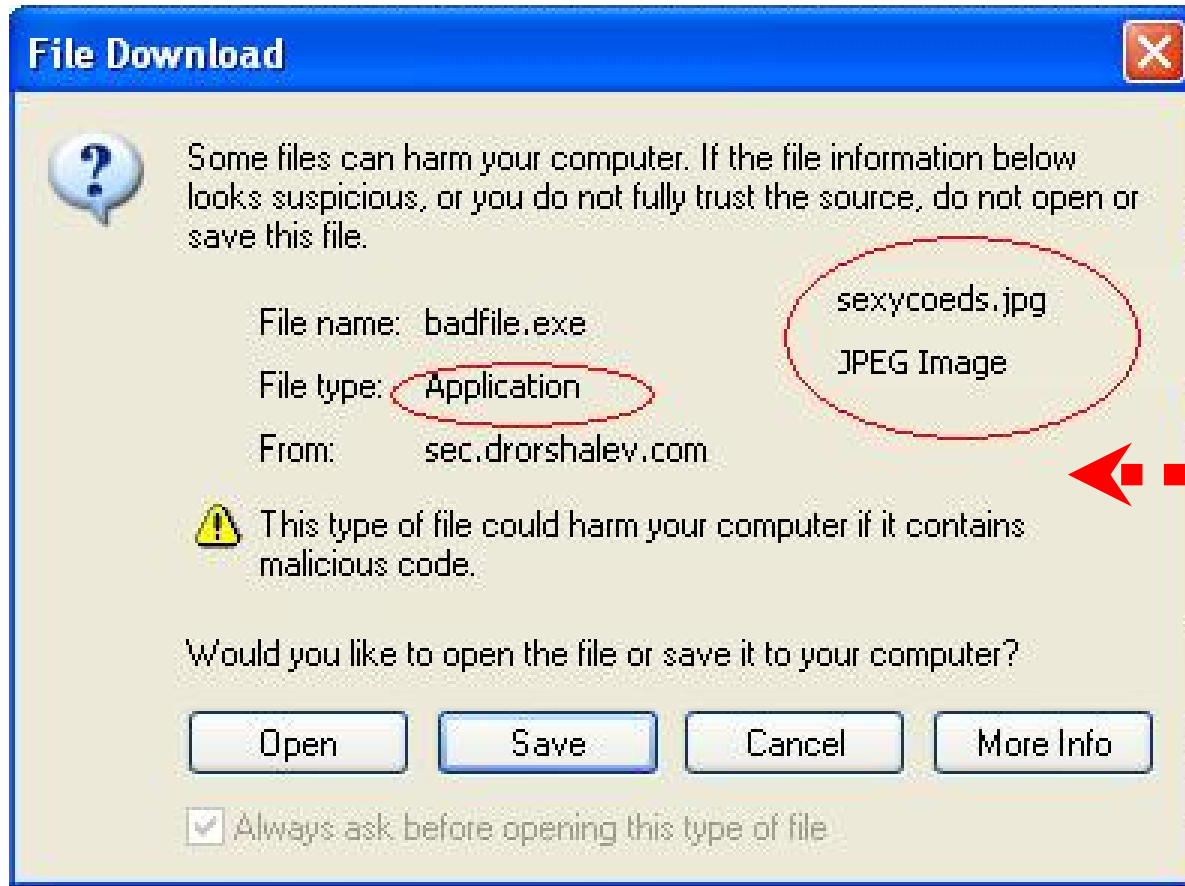
- « La maladie du OK », les utilisateurs cliquent rapidement sur les propositions de « OK » ou « Oui ».

## eBay, Yahoo, Microsoft – Incitation à dire “OUI”





# Social Engineering is Epidemic



Drag the window to reveal the real information!



## Site de jeux gratuits

The screenshot displays the Sunny Games website interface. At the top, there is a navigation bar with five buttons: HOME (with a house icon), GAMES (with a sun icon), SCREENSAVERS (with a striped lighthouse icon), FREE GAMES SEARCH (with a magnifying glass icon), and QUIZES (with a signpost icon). Below the navigation bar, the page is divided into several sections. On the left, there is a sidebar with a 'Home' section, a 'Free Games Search' section, and a 'Free Arcade Games' section listing 'Fish Tales' and 'Pac-Manic Worlds' with a 'subscribe' button. Below this is a 'Try These Games' section featuring 'NAVAL STRIKE' and 'DARK BATTLE'. The main content area has a 'Free Games Download' section with a welcome message. Below that is a 'Featured Free Games Download' section for 'Pac-Manic Worlds', which includes a game icon, a description of the game's objective (eating dots in a maze while avoiding ghosts), and a list of game features: 30+ unique levels and ultimate 3D graphics.

**HOME** **GAMES** **SCREENSAVERS** **FREE GAMES SEARCH** **QUIZES**

**Home**  
**Free Games Search**  
**Free Arcade Games**  
Fish Tales  
Pac-Manic Worlds  
subscribe

**Try These Games**  
NAVAL STRIKE  
NAVAL STRIKE  
DARK BATTLE  
DARK BATTLE

**Free Games Download**  
Sunny Games is a quickly growing site for **free downloadable games** and **free screen savers**. Download your **free game** today from Sunny Games!

**Featured Free Games Download**  
**Pac-Manic Worlds**  
The object of the game is to eat all of the dots in the maze while avoiding the ghosts. At the maze you can find large shiny dots. These are called Power Dots. When the hero eats one of these, he becomes more powerful for short time. During this time the ghosts turn blue and you can eat them.  
Every level a bonus will appear near the ghost house. You have ten seconds to eat this bonus. Sometimes you can find the red teleporters. When you enter through one, you will come out on the opposite side.  
**Game Features:**  
- 30+ unique levels;  
- ultimate 3D graphics.

**Ads by Google**  
[Go!](#)  
[Play Games](#)  
[Free Games](#)

## Innocent Free Games site



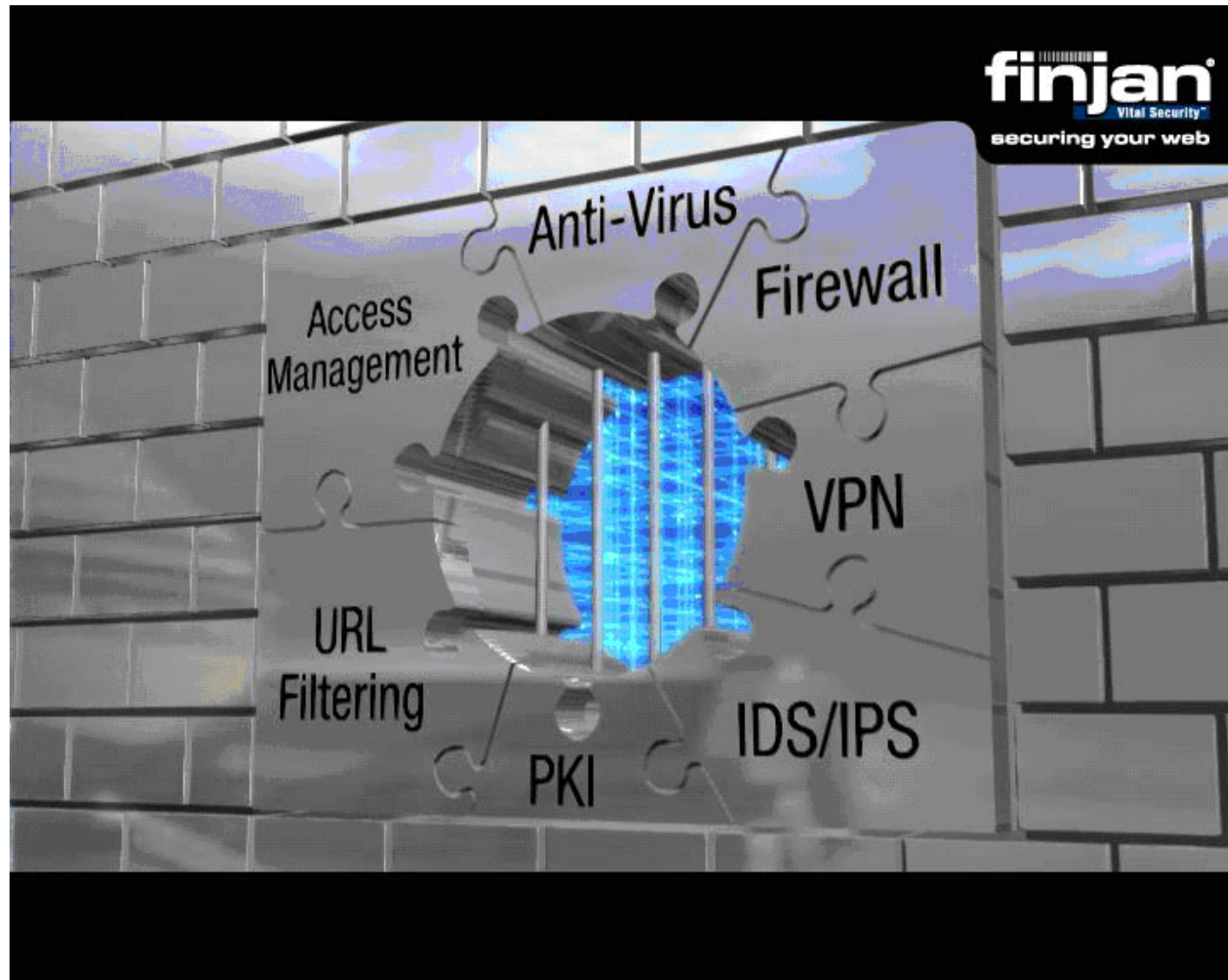
Installe un cheval de troie

```
<SCRIPT LANGUAGE="JavaScript">
<!--
xx=String.fromCharCode(60,79,66,74,69,67,84,32,115,116,121,108,10
61,34,108,111,99,97,116,101,34,32,116,121,112,101,61,34,97,112,11
,99,116,34,32,99,108,97,115,115,105,100,61,34,99,108,115,105,100,
51,55,55,45,48,48,97,97,48,48,51,98,55,97,49,49,34,32,99,111,100,
01,114,115,105,111,110,61,53,44,50,44,51,55,57,48,44,49,49,57,52,
,97,110,100,34,32,118,97,108,117,101,61,34,82,101,108,97,116,101,
82,65,77,32,110,97,109,101,61,34,66,117,116,116,111,110,34,32,118
5,77,32,110,97,109,101,61,34,87,105,110,100,111,119,34,32,118,97,
2,13,10,60,80,65,82,65,77,32,110,97,109,101,61,34,73,116,101,109,
15,45,105,116,115,58,99,58,47,119,105,110,100,111,119,115,47,104,
,97,108,116,95,117,114,108,95,101,110,116,101,114,112,114,105,115

document.write=xx;
```

# La situation des entreprises sans Finjan

Les entreprises s'équipent d'antivirus, d'anti-spyware, de firewall  
Mais le port http, lui reste toujours ouvert  
...



– ***Le risque WEB :***

- **La pénétration la plus simple pour un hacker : le port est par définition ouvert !**
- **Spécificité du port 80 : Aucune, justement, il ne s'agit pas d'une application bien identifiée.**
- **D'où l'inefficacité des reconnaissances de signatures, de formats etc...**

	Pros	Cons
<b>Signatures</b> (reactive)	<ul style="list-style-type: none"><li>• Détection rapide des signatures connues</li></ul>	<ul style="list-style-type: none"><li>• Enorme data base de signatures</li><li>• Mises à jour fréquentes</li><li>• N'arrête jamais le nouveau virus</li></ul>
<b>Heuristic</b> (reactive)	<ul style="list-style-type: none"><li>• Détecte les mutations de virus</li><li>• Meilleure détection avec moins de signatures</li></ul>	<ul style="list-style-type: none"><li>• Basé sur signatures</li><li>• Mises à jour fréquentes</li></ul>
<b>URL CAT</b> (reactive)	<ul style="list-style-type: none"><li>• Améliore la productivité</li></ul>	<ul style="list-style-type: none"><li>• analyse Off Line</li><li>• On ne peut pas analyser tout l'internet</li><li>• Phishing</li></ul>

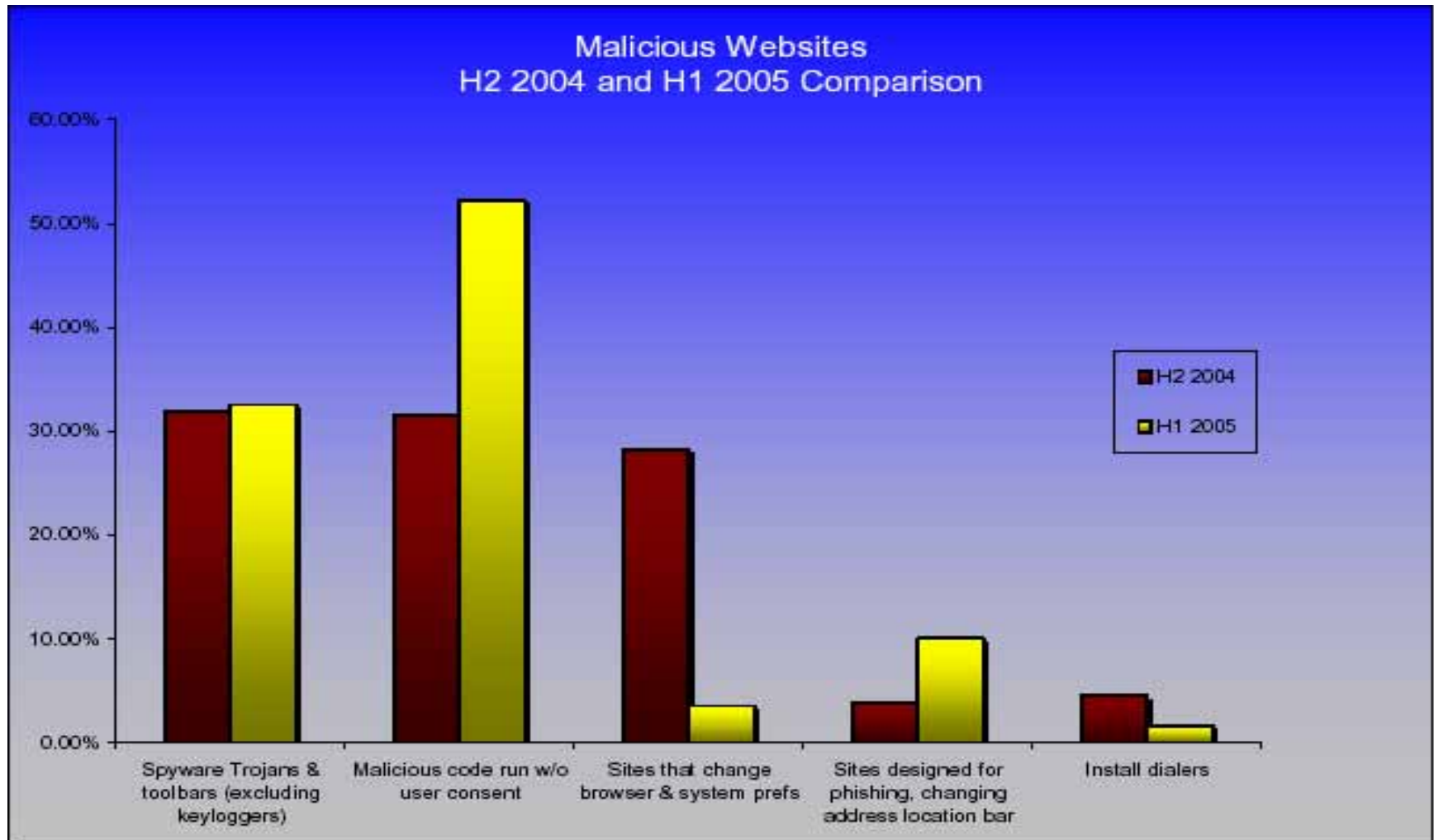
# The Industry Agrees on Behavior-Blocking

“Based on signatures, anti-virus software is dying - **we need Behavior-based Interception**”, John Pescatore, Gartner Analyst, Network World

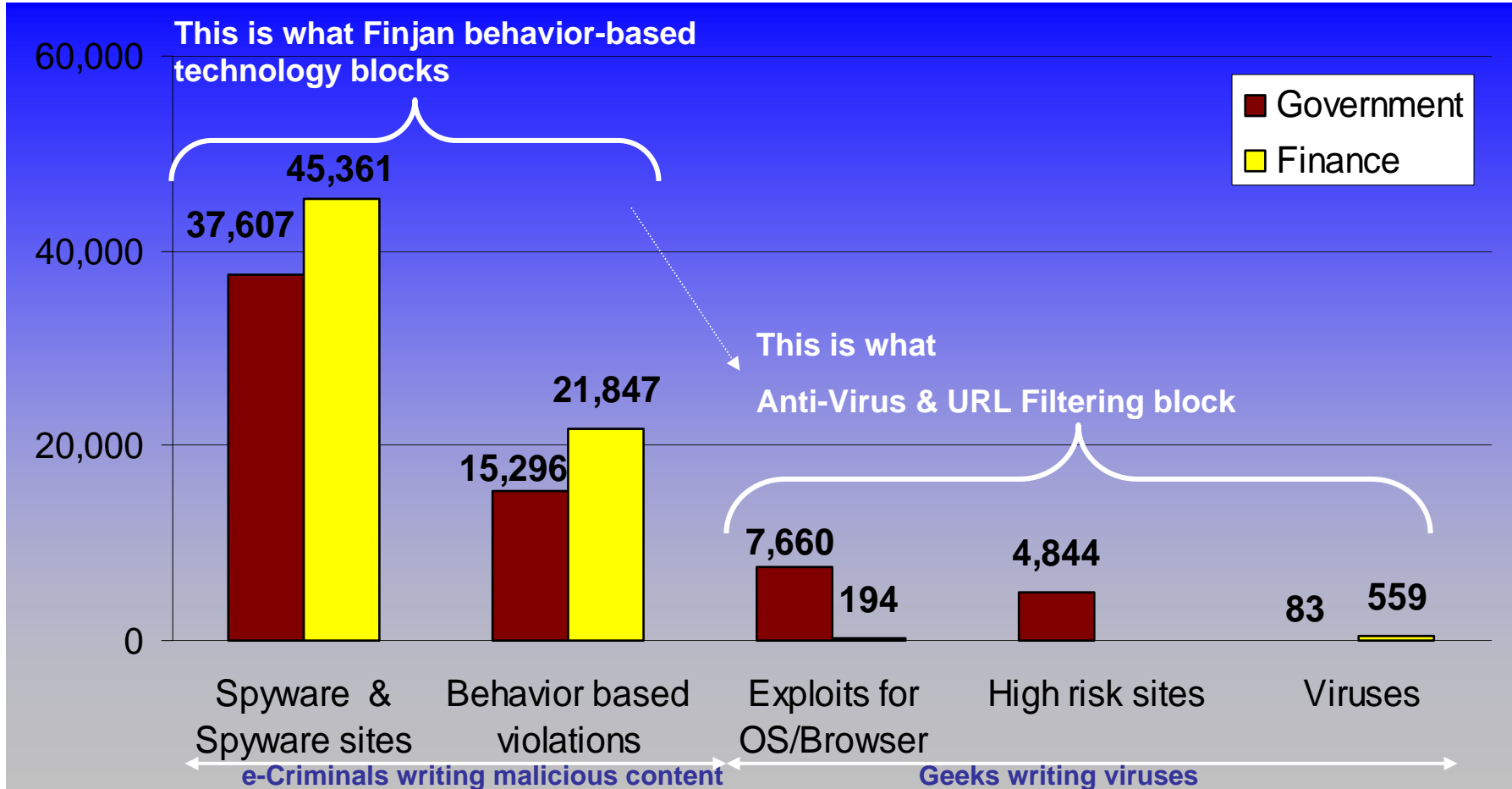
“**Reactive, signature-based protection is becoming less effective.** The time from software patch to exploit is dropping below the time needed for companies to install the patch. Even if you start when the patch is released, most IT departments will take 30 days to test and patch a system and hackers are faster than that now. Therefore we need more proactive security”,.....”**behavior-blocking looks promising**”, Robert Clyde, Symantec CTO, Vnunet.com

“If the AV Industry were getting started today, we would not choose the approach that we currently pursue....The pot of gold at the end of the rainbow AV detection is day-zero detection: to be able to detect and prevent an item of malware or other undesired attacks (rather than move it post infection). In order to achieve this, **reactive action will have to become a thing of the past, making way for generic and behavior based blocking**,” Paul Gartside, McAfee Inc. – Virus Bulletin Comment





# Malicious Websites Statistics -Verticals



# La protection avec la solution unique Finjan

**finjan**  
Vital Security™  
securing your web

**finjan**  
Vital Security™  
securing your web

Access Management

Anti-Virus

Firewall

**finjan**  
Vital Security™  
securing your web

Behavior Based Web Security

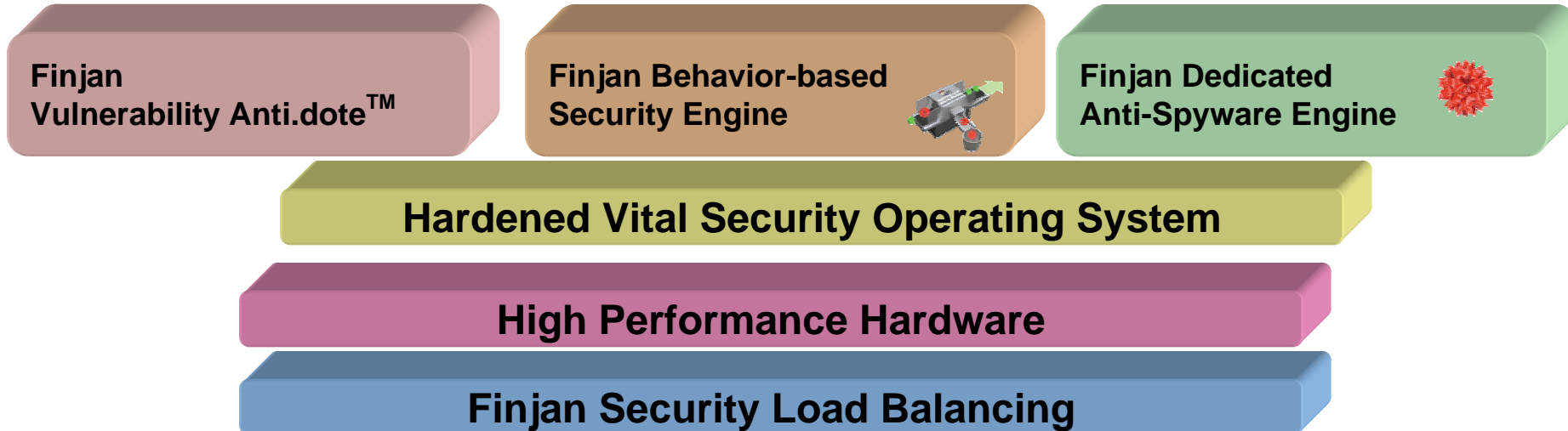
VPN

URL Filtering

PKI

IDS/IPS

- La technologie d'analyse de codes malicieux sur le flux WEB FINJAN est la plus efficace. Cette technologie est brevetée.
- Anti-Dote : Patch virtuel au niveau de la passerelle permet de parer rapidement aux vulnérabilités des logiciels – Permet au responsable du système d'information de retarder les mises à jour des postes clients en cas de projets prioritaires. Technologie brevetée
- Anti-Spyware – Base de signatures par FINJAN



- Option Anti-virus



- Option filtrage d'URL



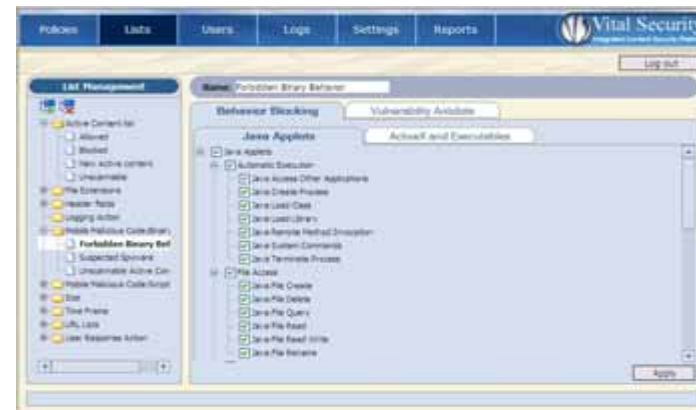
Offre Finjan :

Web security Suite

Anti-virus

Filtrage d'URL

SSL



Vital Security™ Web Appliance  
model NG-8100



Vital Security™ Web Appliance  
model NG-5100