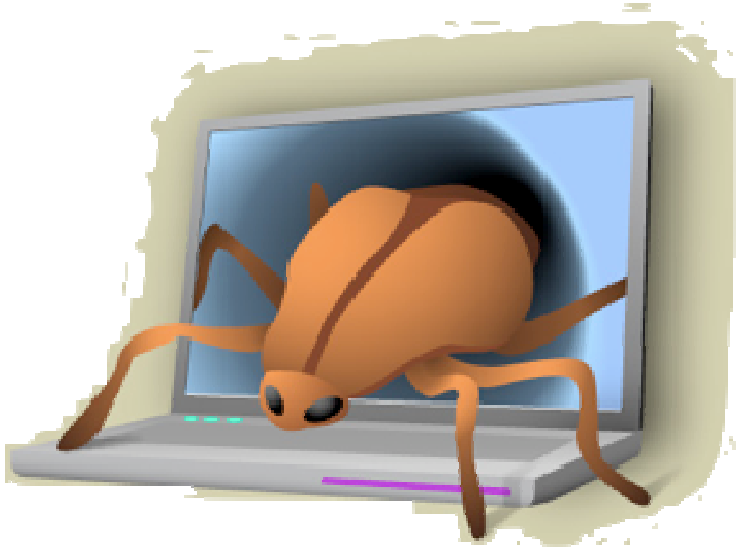
بدافزار
(Malware)

رئوس مطالب

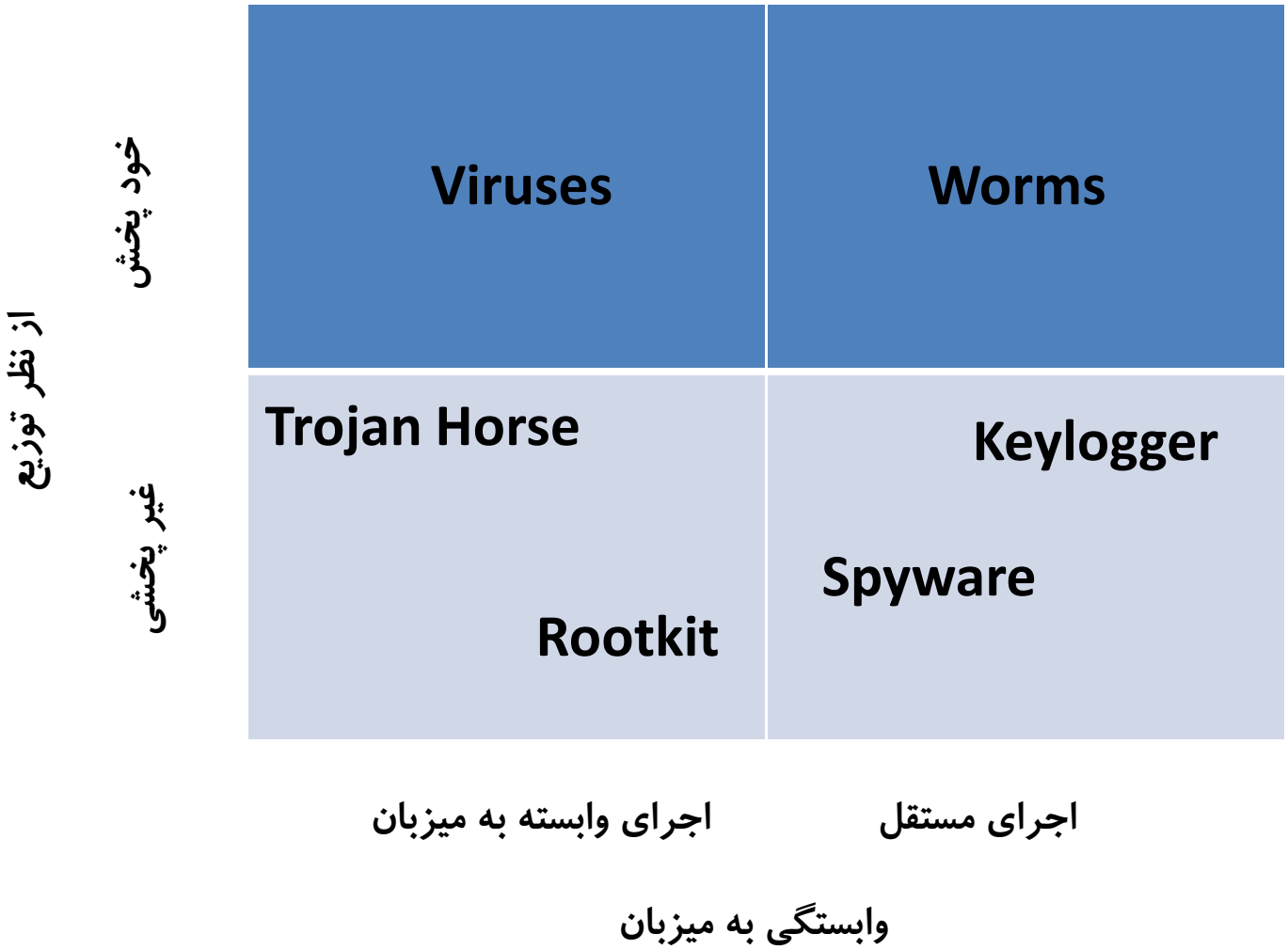
- بدافزار
- روش های آلوده کردن
- روش های تکثیر شدن
- روش های شناسایی

بدافزار

- برنامه ای است که روی کامپیوتر قربانی اجرا می شود و عملیاتی را انجام می دهد که مهاجم می خواهد.
  - دزدیدن اطلاعات
  - حذف فایل ها
  - استفاده از کامپیوتر قربانی به عنوان relay



انواع بدافزارها



تعاریف

- ویروس
  - برنامه ای که با تغییر برنامه های دیگر آن ها را آلوده کرده تا کارکردهای برنامه قربانی را به نفع خود تغییر دهد.
    - ویروس های چند ریختی (Polymorphic): از الگوریتم های چند ریختی برای تغییر امضاء خود بهره می برند به قسمی که کارکردشان تغییر نکند.
    - ویروس های دگردیس (Metamorphic): بعد از هر آلودگی امضاء آن ها تغییر می یابد.
- تروجان
  - برنامه ای است که در ظاهر قصد انجام عملی مطلوب را دارد و در حقیقت در پشت پرده عملیاتی بدخواهانه را با دسترسی غیر مجاز انجام می دهد.

تعاریف (ادامه)

- روت کیت
  - برنامه ای است که از تکنیک های نهانکاری برای حضور همیشگی روی کامپیوتر قربانی بدون اینکه شناسایی شود، بهره می برد.
- کرم
  - برنامه ای است که به طور خودکار خود را کپی می کند و از شبکه برای ارسال کپی های خود به دیگر کامپیوترها استفاده می کند.
- جاسوس افزار
  - برنامه ای است که بدون رضایت کاربر روی کامپیوتر اجرا می شود و وظیفه قاپیدن اطلاعات و کنترل کردن کامپیوتر قربانی را برعهده دارد.

انواع جاسوس افزار

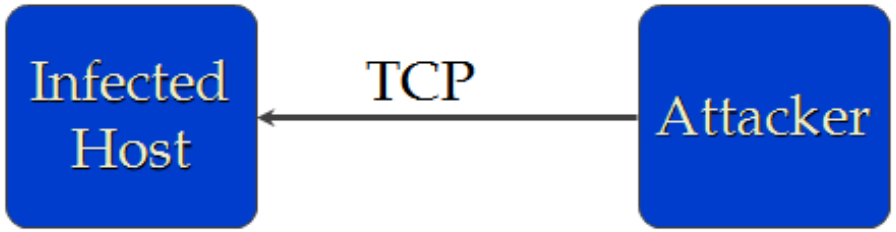
- Adware
  - برنامه ای که مطالب تبلیغاتی را به طور خودکار دانلود کرده و نشان می دهد.
- Collectware
  - برنامه ای است الگوی رفتاری کاربران وب را استخراج می کند و به صورت اطلاعات آماری در اختیار مهاجم قرار می دهد.
  - این اطلاعات بعداً به شرکت های تبلیغاتی فروخته می شود.

انواع جاسوس افزار (ادامه)

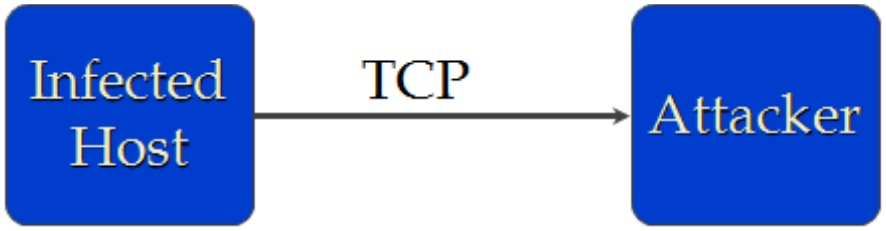
- Keyloggers
  - برنامه هایی که روی کامپیوتر قربانی نصب می شوند و کلید زده شده توسط کاربر را ثبت می کنند. سپس مهاجم اطلاعاتی از قبیل پسورد و شماره حساب ها را استخراج می کنند.

درب پشتی

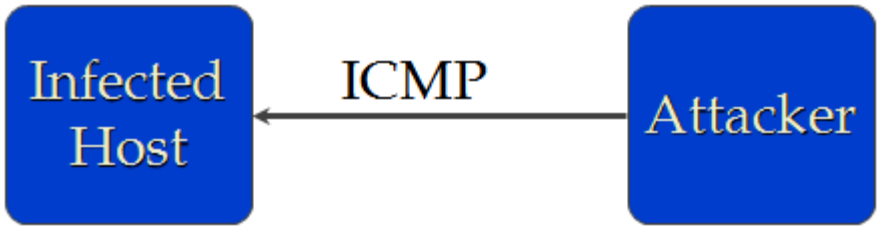
- Basic



- Reverse

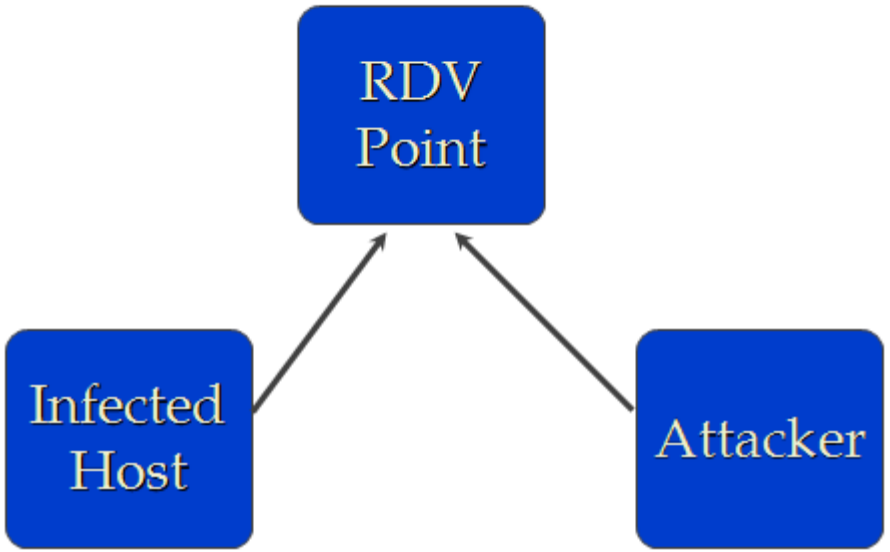


- Covert

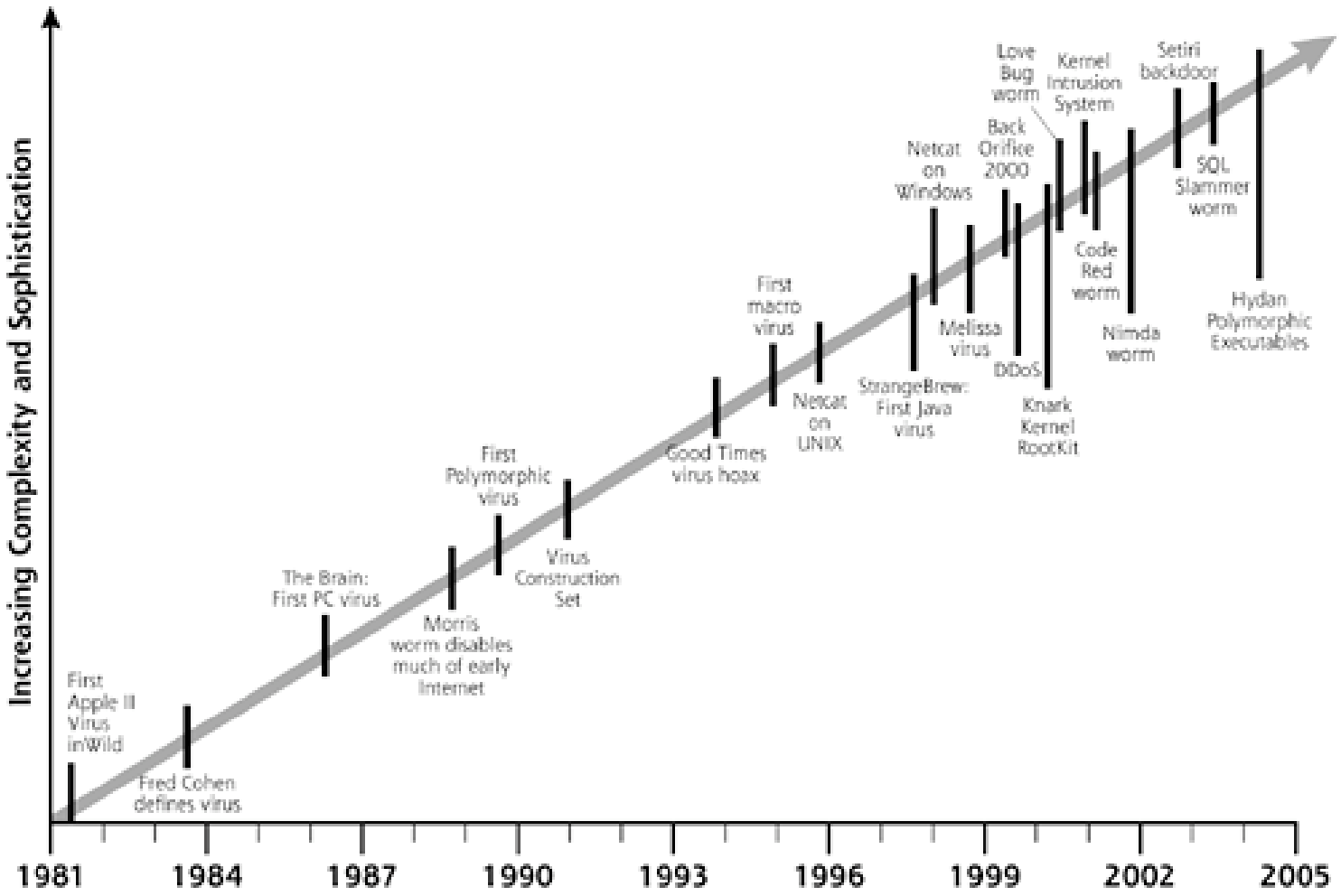


درب پشتی (ادامه)

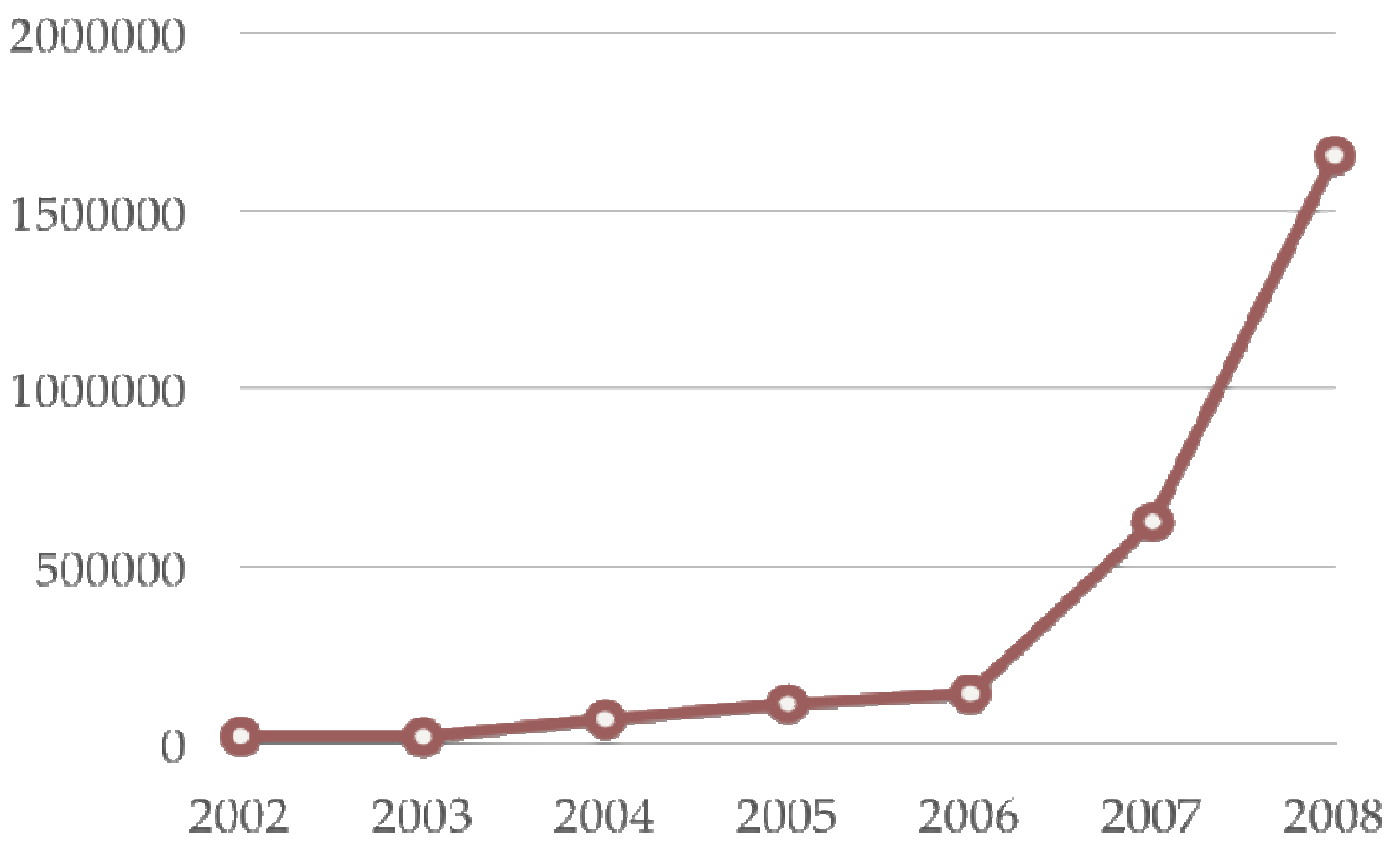
- Rendezvous



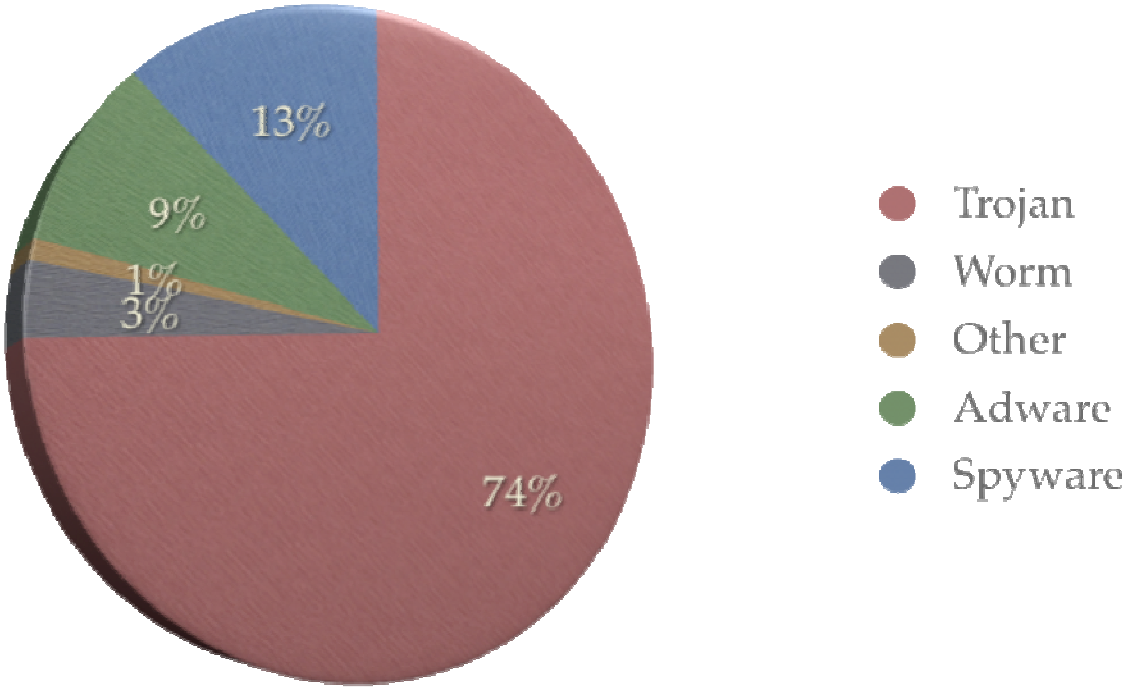
تاریخچه بدافزارها



تعداد امضاء های بدافزارها



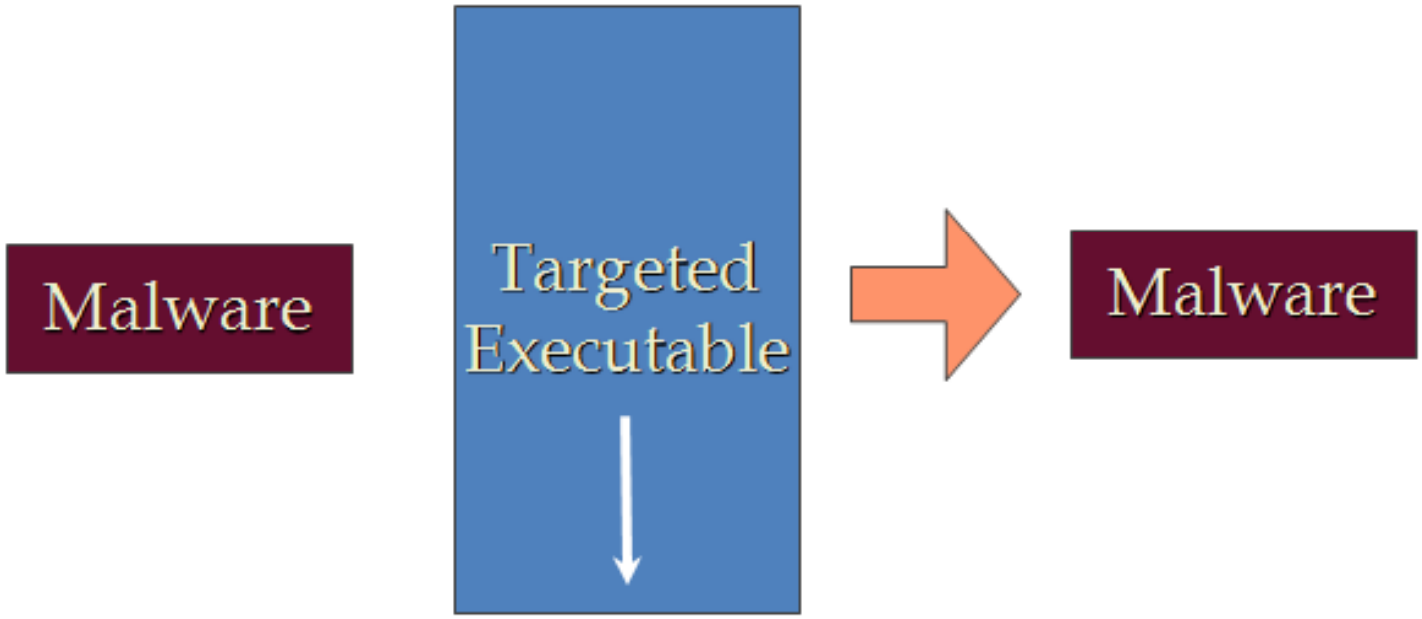
تقسیم بندی بدافزارها



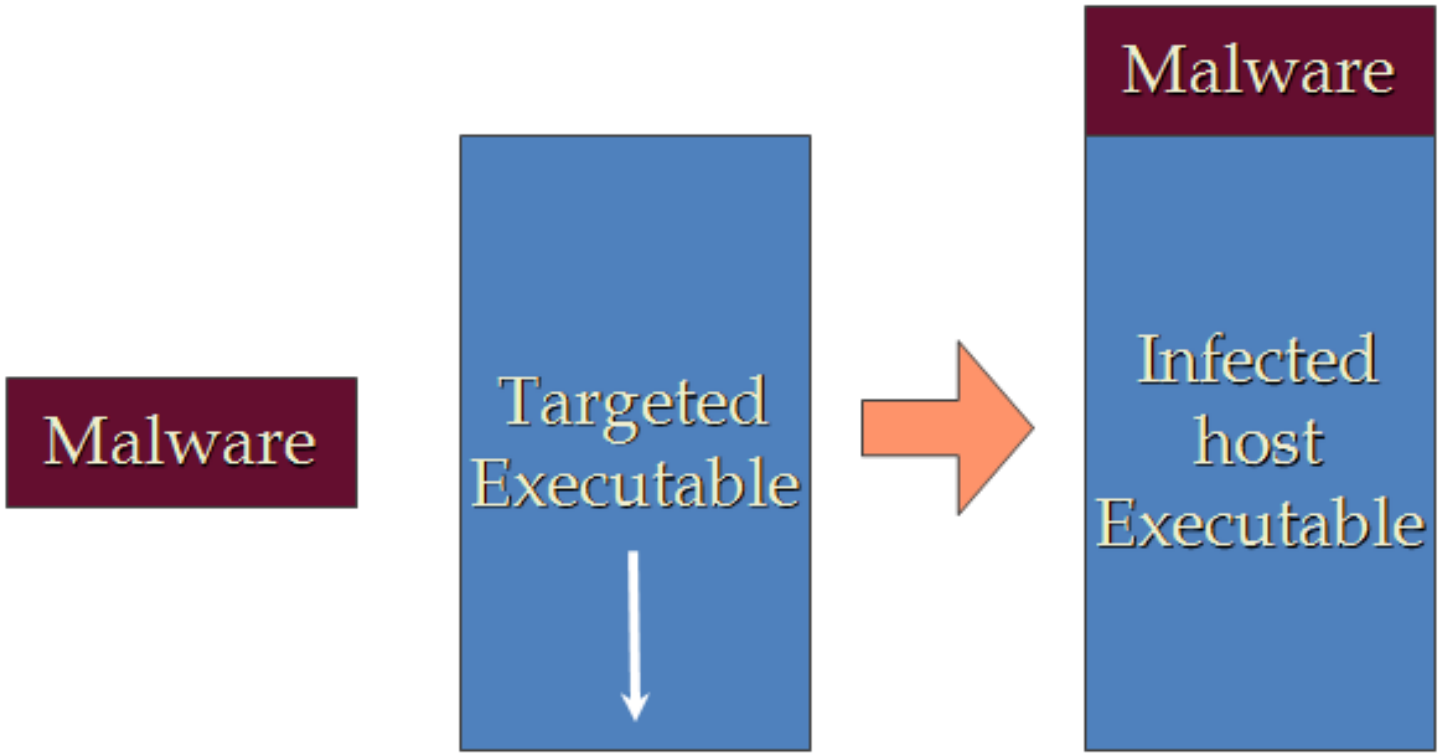
چه چیزی آلوده می شود؟

- Executable
- Interpreted file
- Kernel
- MBR
- Hypervisor

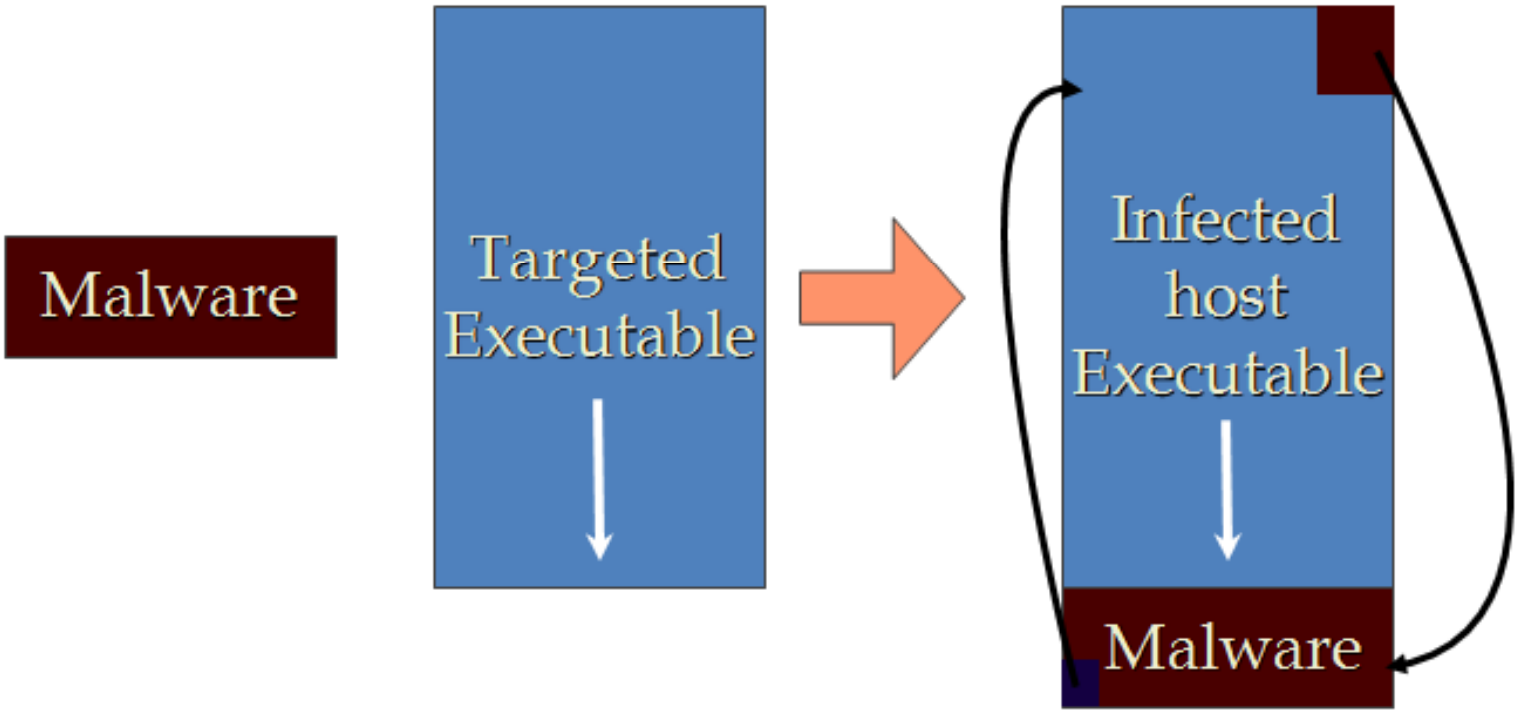
Overwriting Malware



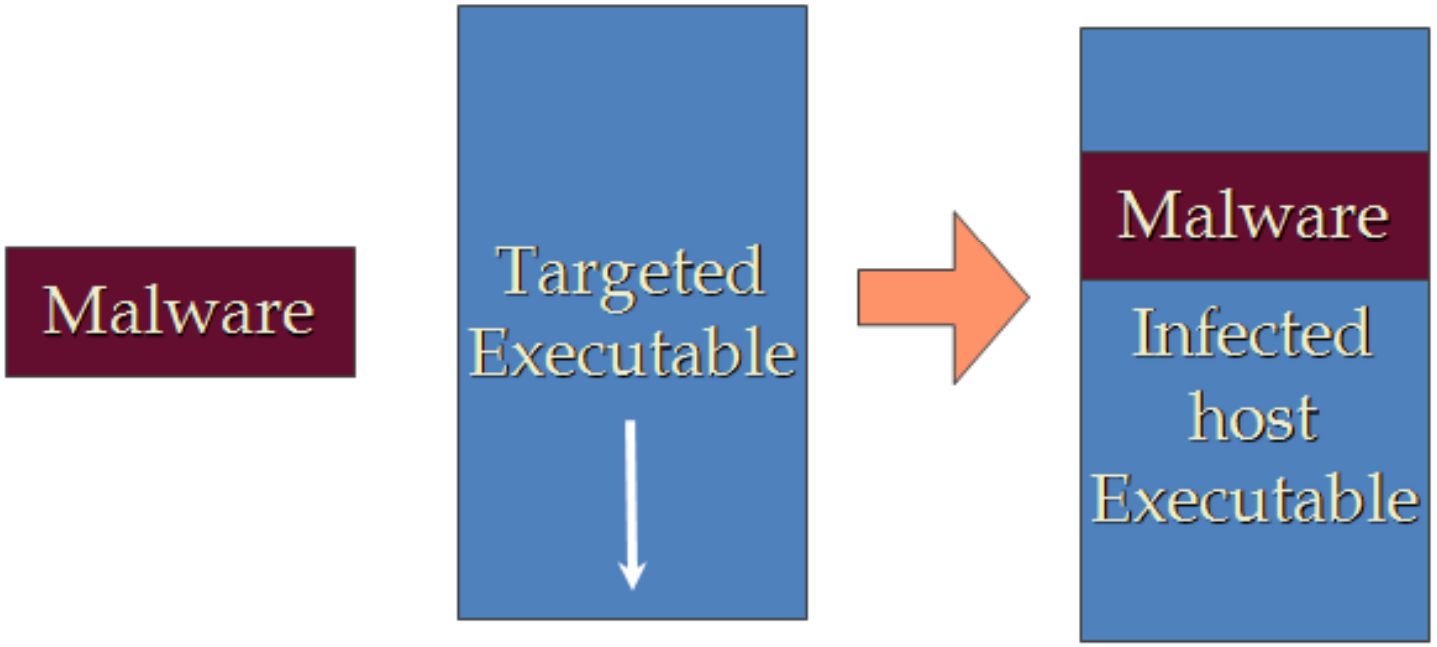
Prepending Malware



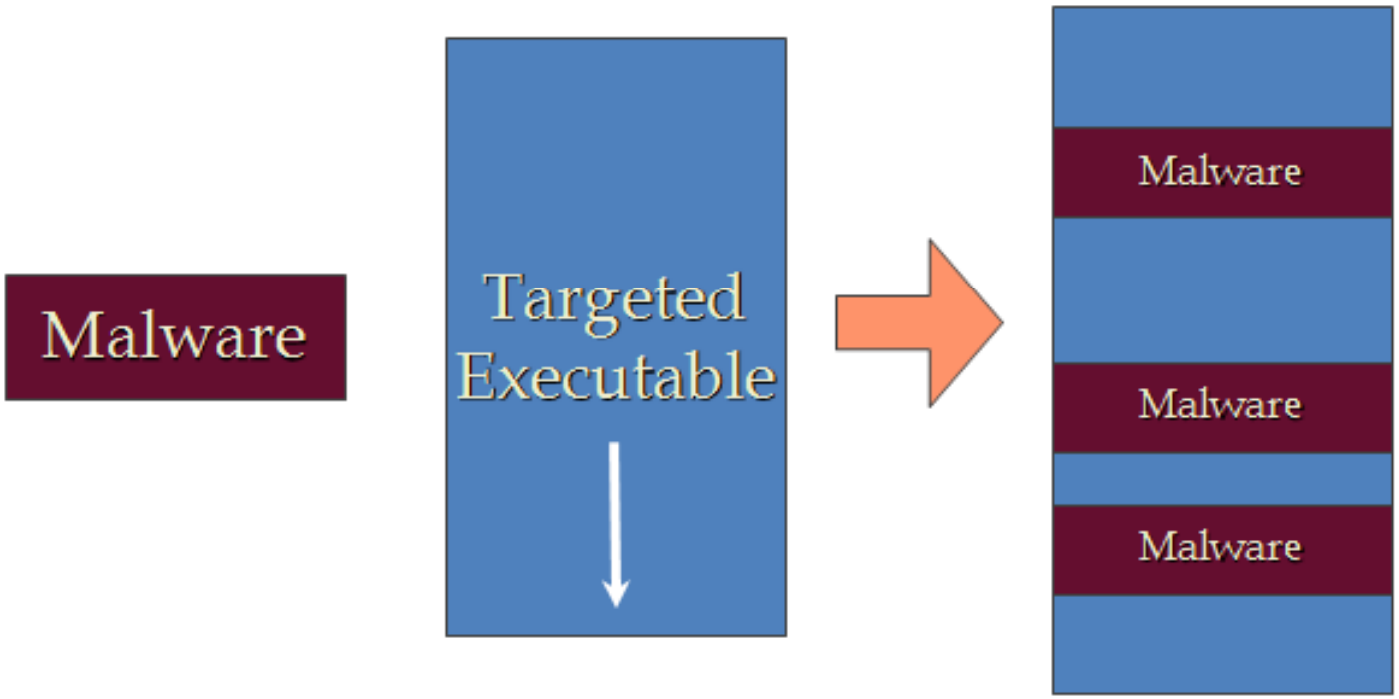
Appending Malware



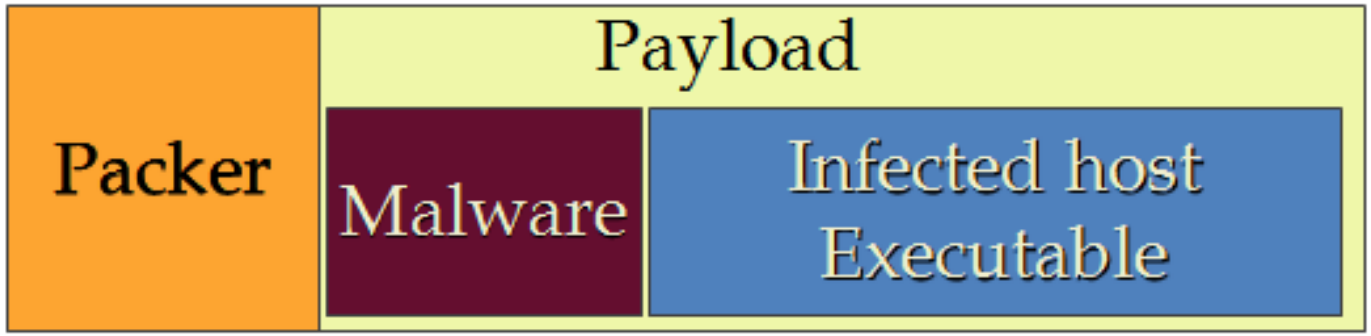
Cavity Malware



Multi-Cavity Malware



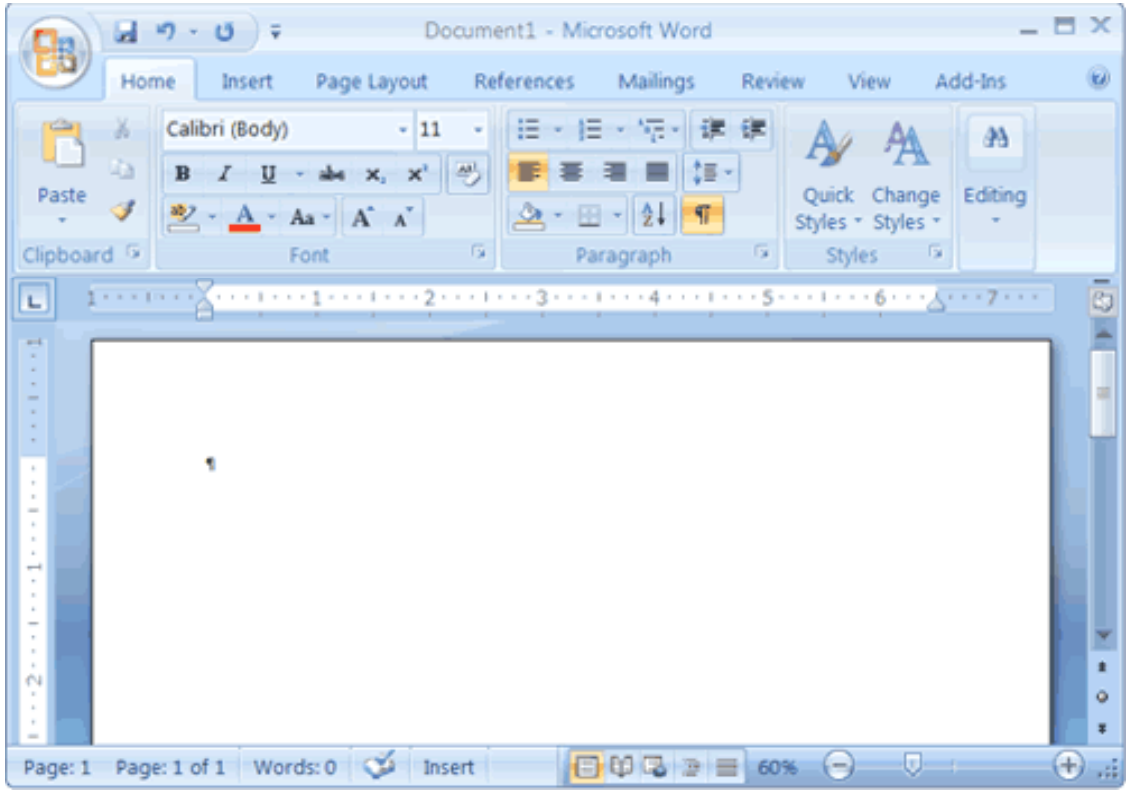
Packers



کارکردهای Packer

- فشرده کردن (Compress)
- رمز کردن (Encrypt)
- تصادفی کردن (چند ریختی)
- Anti-debug
- Anti-VM

Document-based Malwares



- MS-Office
- Acrobat

روش های تکثیر شدن

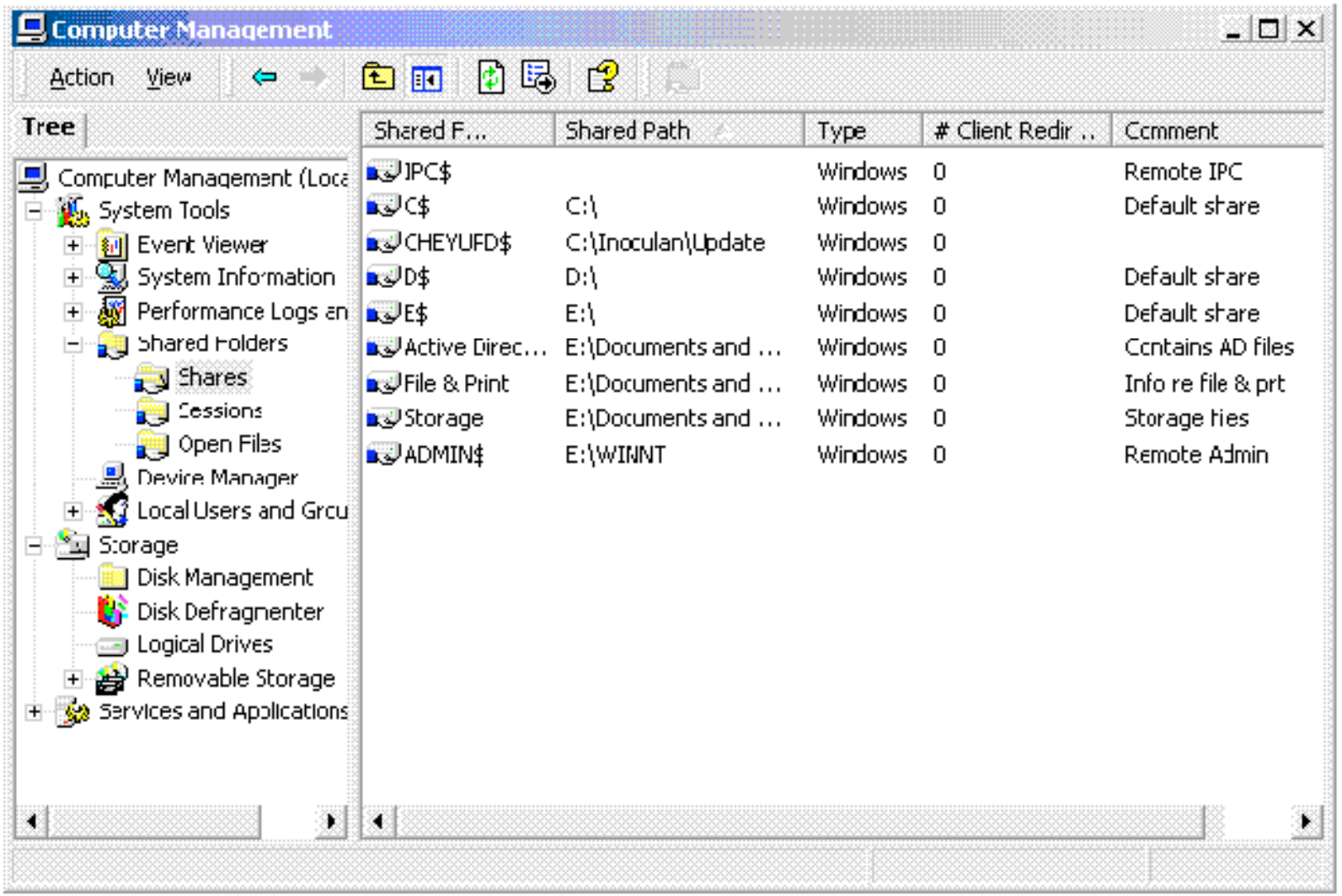
روشهای تکثیر

- استفاده از حفره های امنیتی در سیستم های کامپیوتری در شبکه، مانند:
  - Buffer overflow
  - Dictionary attacks
- از طریق دانلود
  - دانلود از طریق وب و اجرا بر روی ماشین قربانی
  - استفاده غیر مجاز از plugin های وب
  - حفره های امنیتی در web browser

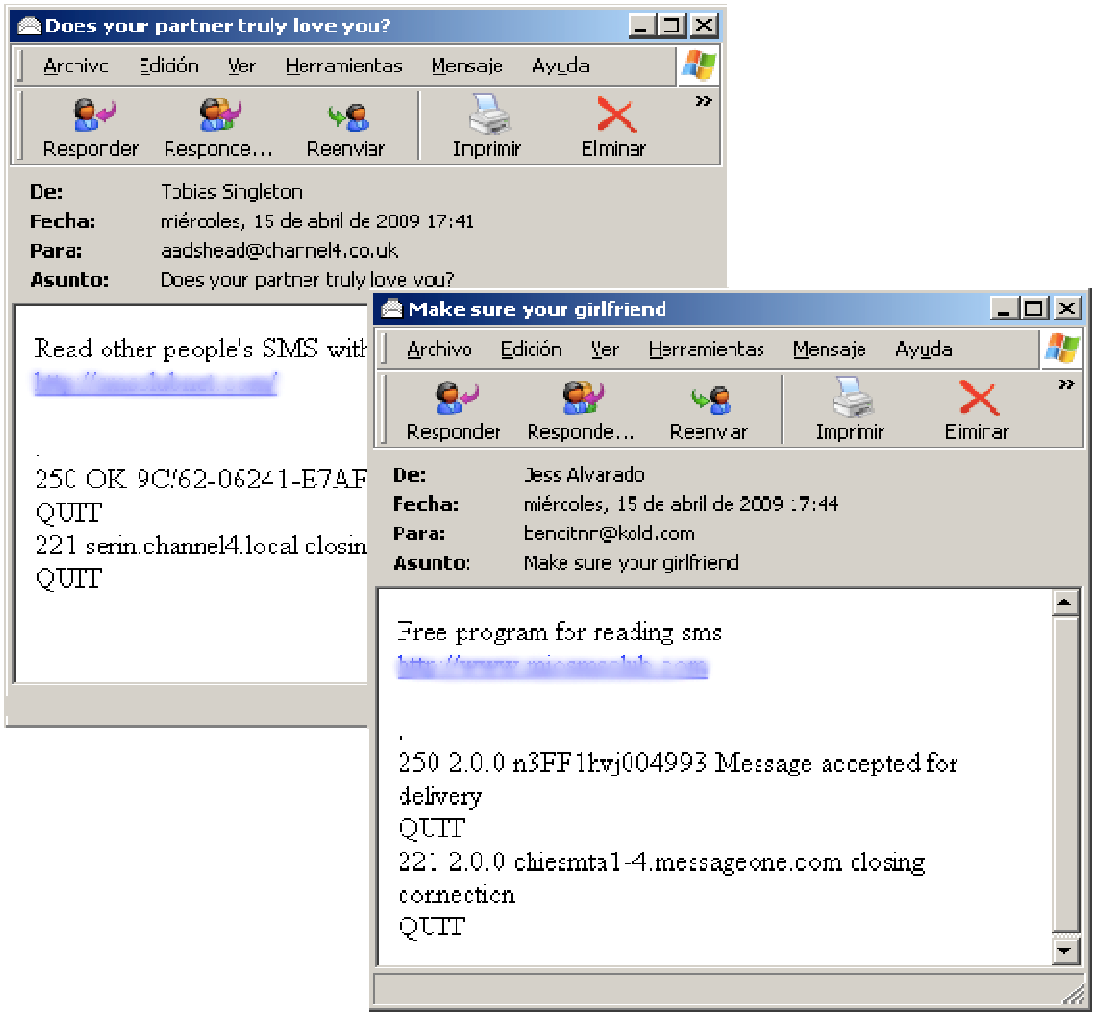
روشهای تکثیر

- مهندسی اجتماعی
  - از طریق تحریک کاربر

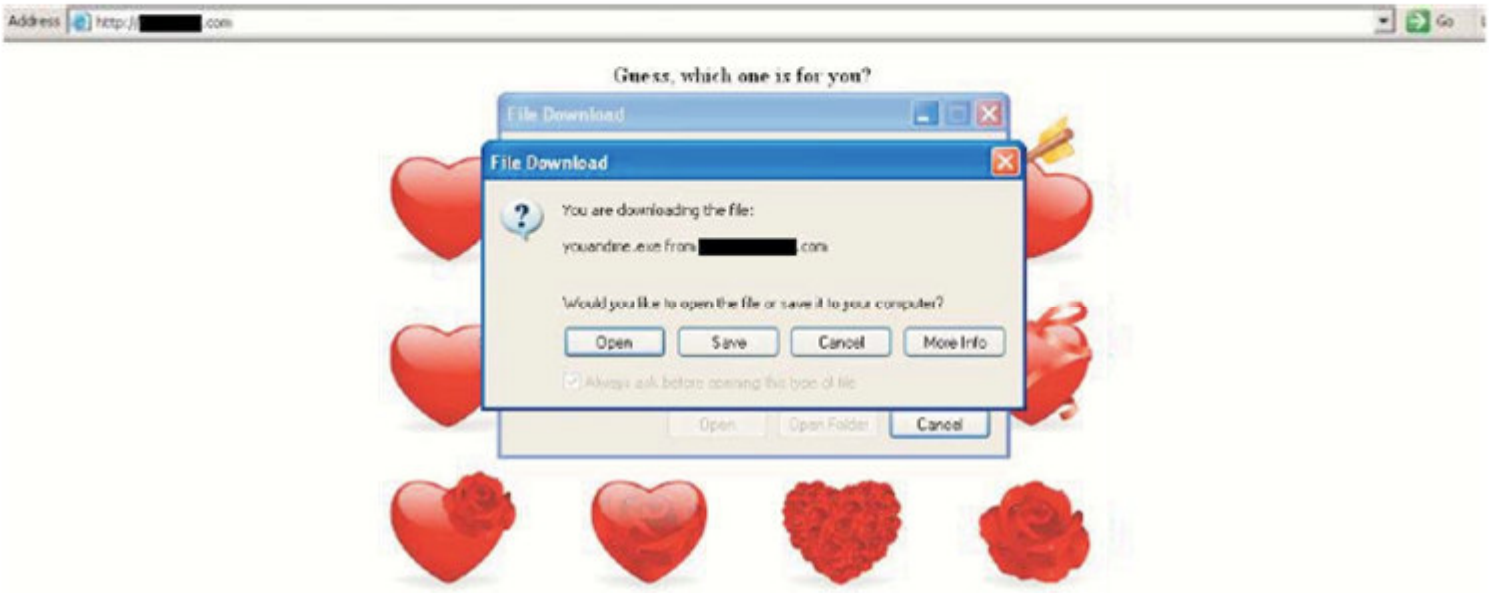
Shared Folders



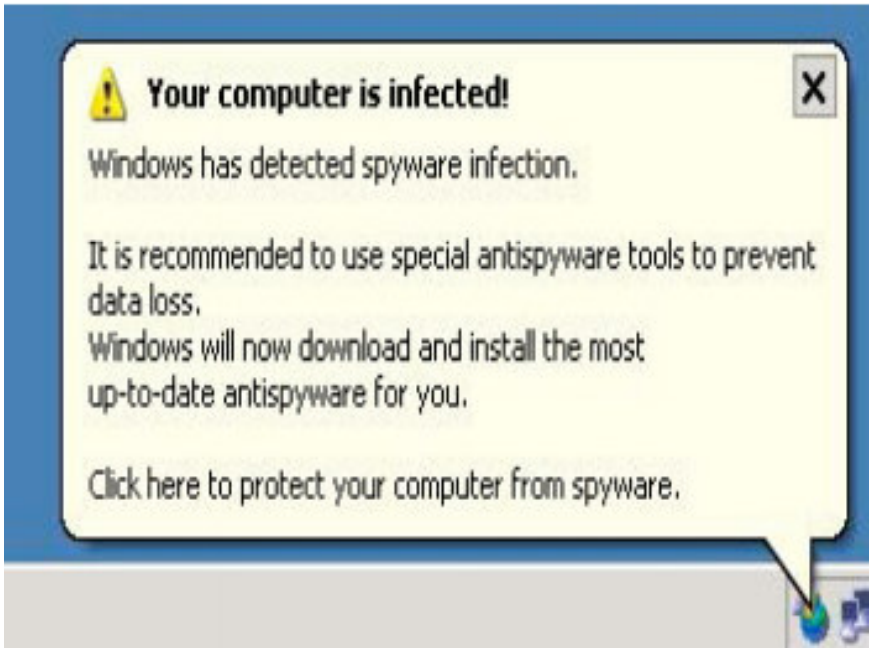
Email


Does your partner truly love you?
Archivo Edición Ver Herramientas Mensaje Ayuda
Responder Responde... Reenviar Imprimir Eliminar
De: Tobias Singleton
Fecha: miércoles, 15 de abril de 2009 17:41
Para: aadshead@channel4.co.uk
Asunto: Does your partner truly love you?
Read other people's SMS with
250 OK 9C762-06241-E7AF
QUIT
221 serin.channel4.local closin
QUIT
Make sure your girlfriend
Archivo Edición Ver Herramientas Mensaje Ayuda
Responder Responde... Reenvar Imprimir Eimirar
De: Jess Alvarado
Fecha: miércoles, 15 de abril de 2009 :7:44
Para: bencitnr@kold.com
Asunto: Make sure your girlfriend
Free program for reading sms
250 2.0.0 n3FF1kvj004993 Message accepted for delivery
QUIT
221 2.0.0 chiesmta1-4.messageone.com closing connection
QUIT

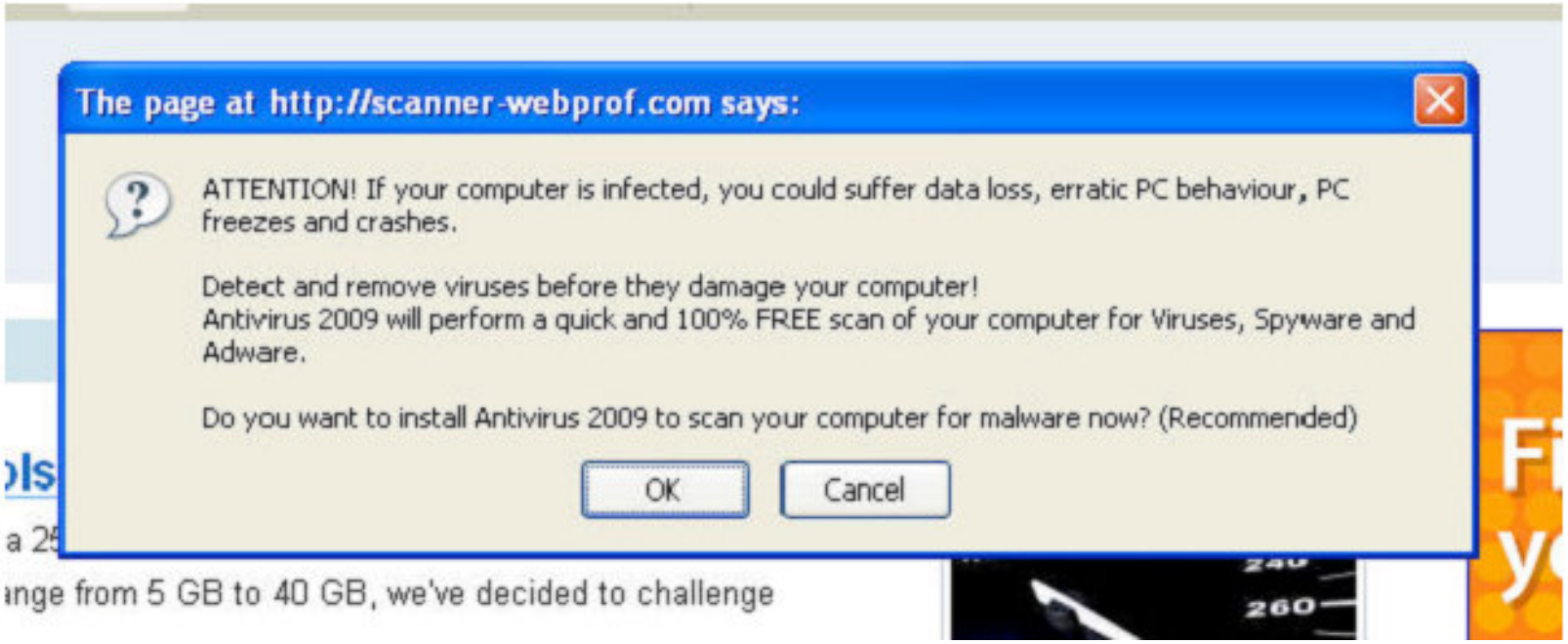
Valentine Day



Fake Antivirus

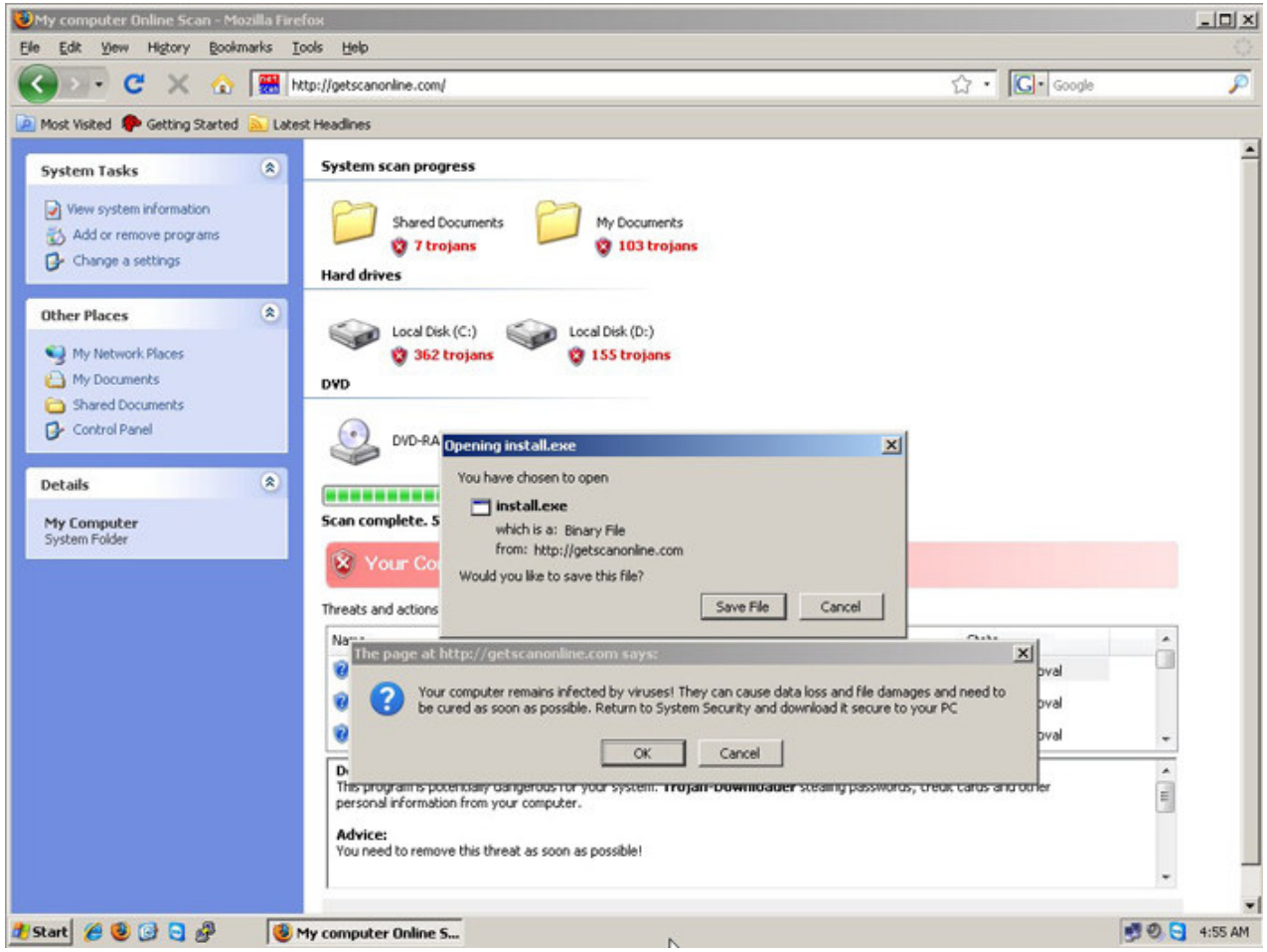


Pop-ups

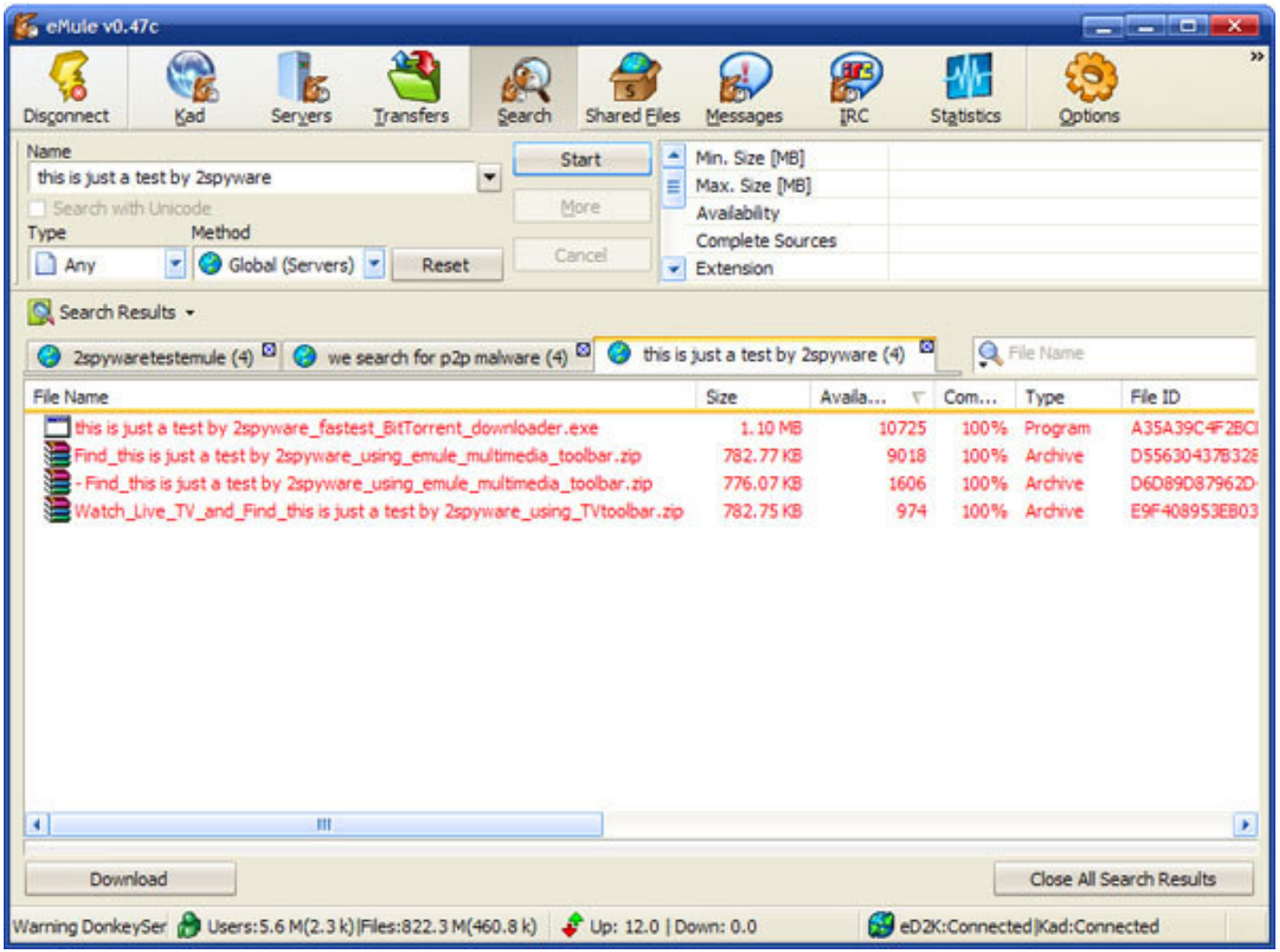

The page at http://scanner-webprof.com says:
ATTENTION! If your computer is infected, you could suffer data loss, erratic PC behaviour, PC freezes and crashes.
Detect and remove viruses before they damage your computer!
Antivirus 2009 will perform a quick and 100% FREE scan of your computer for Viruses, Spyware and Adware.
Do you want to install Antivirus 2009 to scan your computer for malware now? (Recommended)
OK
Cancel
ange from 5 GB to 40 GB, we've decided to challenge

Hijack Browser

Fake Page


My computer Online Scan - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://getscanonline.com/
Most Visited Getting Started Latest Headlines
System Tasks
View system information
Add or remove programs
Change a settings
Other Places
My Network Places
My Documents
Shared Documents
Control Panel
Details
My Computer
System Folder
System scan progress
Shared Documents
7 trojans
My Documents
103 trojans
Hard drives
Local Disk (C:)
362 trojans
Local Disk (D:)
155 trojans
DVD
DVD-RA
Opening install.exe
You have chosen to open
install.exe
which is a: Binary File
from: http://getscanonline.com
Would you like to save this file?
Save File
Cancel
Scan complete. S
Your Co
Threats and actions
The page at http://getscanonline.com says:
Your computer remains infected by viruses! They can cause data loss and file damages and need to be cured as soon as possible. Return to System Security and download it secure to your PC
OK
Cancel
personal information from your computer.
Advice:
You need to remove this threat as soon as possible!
Start
My computer Online S...
4:55 AM

P2P Files


eMule v0.47c
Disconnect
Kad
Servers
Transfers
Search
Shared Files
Messages
IRC
Statistics
Options
Name
this is just a test by 2spyware
Search with Unicode
Type
Any
Method
Global (Servers)
Reset
Start
More
Cancel
Min. Size [MB]
Max. Size [MB]
Availability
Complete Sources
Extension
Search Results
2spywaretestemule (4)
we search for p2p malware (4)
this is just a test by 2spyware (4)
File Name
File Name
Size
Availa...
Com...
Type
File ID
this is just a test by 2spyware_fastest_BitTorrent_downloader.exe 1.10 MB 10725 100% Program
Find_this is just a test by 2spyware_using_emule_multimedia_toolbar.zip 782.77 KB 9018 100% Archive
- Find_this is just a test by 2spyware_using_emule_multimedia_toolbar.zip 776.07 KB 1606 100% Archive
Watch_Live_TV_and_Find_this is just a test by 2spyware_using_TVtoolbar.zip 782.75 KB 974 100% Archive
Download
Close All Search Results
Warning DonkeySer
Users:5.6 M(2.3 k)|Files:822.3 M(460.8 k)
Up: 12.0 | Down: 0.0
eD2K:Connected|Kad:Connected

روش های شناسایی

- آنتی ویروس
  - تحلیل رفتار سیستم
  - تحلیل کد باینری برنامه های اجرایی
- امضاء ویروس
  - شناسایی رشته ای در کد باینری ویروس
- Anti-packer
  - اجرای برنامه و گرفتن محتویات باینری واقعی از حافظه

روش های شناسایی (ادامه)

- تحلیل رفتار برنامه
  - دسترسی به شبکه، فایل های باز، حذف فایل، تغییر سکتور بوت
- Checksum
  - تولید checksum برای فایل های باینری و فایل های پیکربندی
  - شناسایی تغییر با استفاده از مقایسه کردن checksumها
- تحلیل با استفاده از Sandbox
  - اجرای فایل باینری در VM
  - مانیتور کردن فعالیت روی فایل ها، شبکه و حافظه

Tunneling viruses

- برای پائین آوردن احتمال شناسائی ویروس ها از تکنیک های مختلفی استفاده می کنند.
- ویروس های tunneling خود را به جای وقفه های bios قرار می دهند لذا حتی قبل از سیستم عامل اجرا شده و ویروس یاب ها را هم تحت کنترل خواهند داشت.

ویروس های مستتر

- بعضی از ویروس ها خود را به جای برنامه هائی که در لیست ignore ویروس یاب ها هستند جا می زند.
- بخش کوچک و غیر رمز شده از ویروس کدهای برنامه های معروفی مثل notepad در خود دارد. زیرا ویروس یاب ها patternهائی را که در برنامه های خوب و معروف وجود دارد دور می ریزند.

NTFS ADS viruses

- NTFS شامل یک فراخوانی سیستمی به نام Alternate Data Streams(ADS) است که فایل های دانلودی از اینترنت را ذخیره می کند.
- اکثر دستورالعمل های سیستم عامل با فایل های ADS کار نمی کند.
- فایل های ذخیره شده دیده نمی شود، deleteنمی شوند..
- بدافزار ها برای مخفی شدن از این استفاده می کنند.
- ابزار streams.exe از شرکت sysinternals.com برای پیدا کردن این فایل ها مورد استفاده قرار می گیرد.

ویروس های چند ریختی و دگردیس

- ویروس چند ریخت(code packing)
  - ویروس در هر الوده گی تغییر شکل می دهد
  - Payload رمز می شود
  - برای تغییر شکل از کلید های مختلف استفاده می شود
  - آنالیز استاتیک کدها سخت می شود.
  - روتین رمز نگاری باید تغییر شکل دهد تا از این طریق قابل شناسائی نباشد.

دگردیس

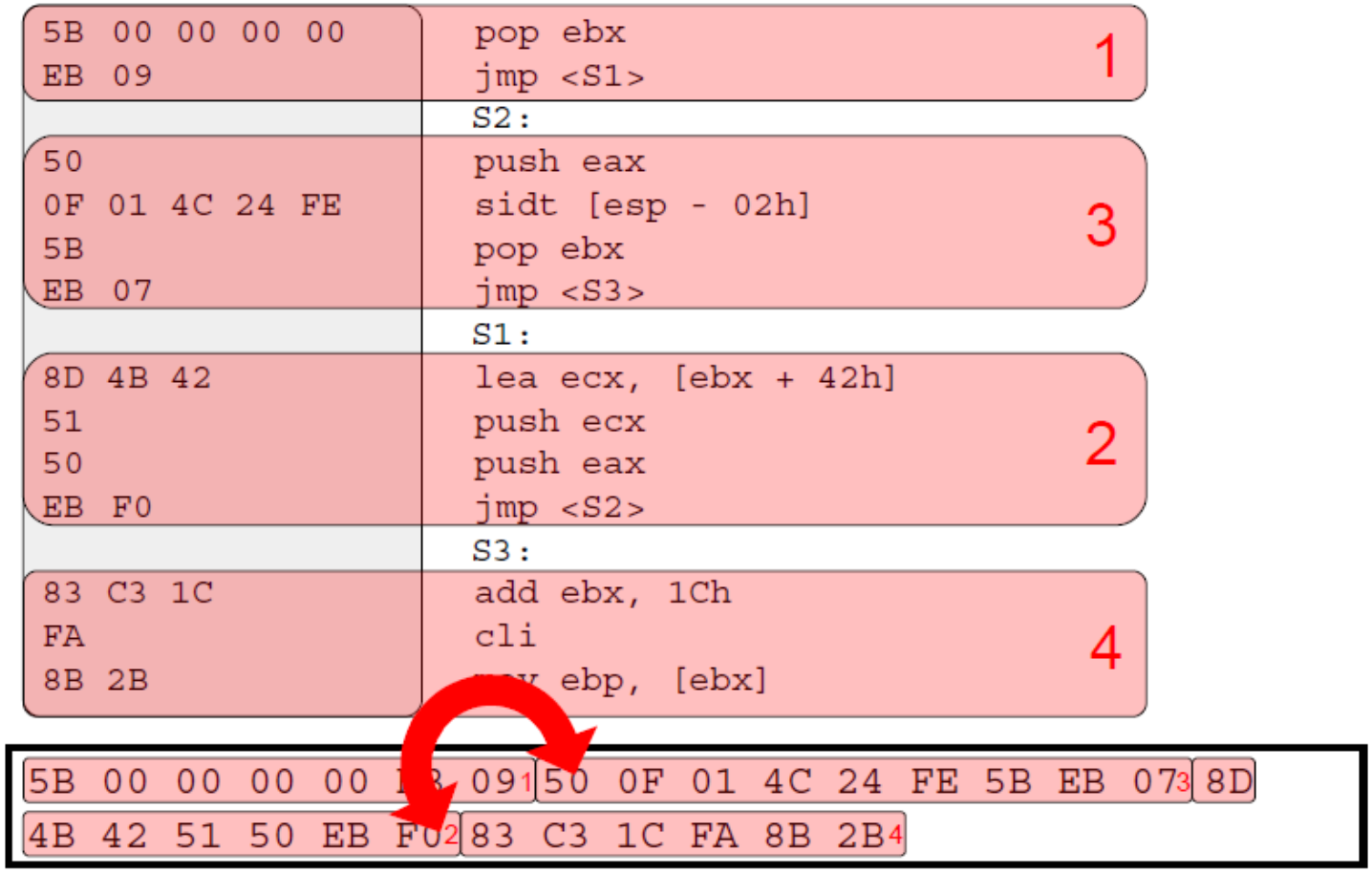
- نسخه های متعدد از یک کد برنامه بد افزار تولید می شود ولی بد افزار از لحاظ semantic همان کار را انجام می دهد.
- روش های مختلف برای تولید نسخه های متفاوت
  - Dead Code Insertion –
  - Instruction Reordering –
  - Instruction Substitution –

تزریق کد مرده

```
5B 00 00 00 00    pop ebx
8D 4B 42          lea ecx, [ebx + 42h]
51                push ecx
50                push eax
90                nop
50                push eax
40                inc eax
0F 01 4C 24 FE    sidt [esp - 02h]
48                dec eax
5B                pop ebx
83 C3 1C          add ebx, 1Ch
FA                cli
8B 2B             mov ebp, [ebx]
```

```
5B 00 00 00 00 8D 4B 42 51 50 90 50 40 0F 01 4C 24 FE
48 5B 83 C3 1C FA 8B 2B
```

جابجائی کدها



جایگزینی دستورات

```
5B 00 00 00 00    pop ebx
8D 4B 42          lea ecx, [ebx + 42h]
51                push ecx
50                push eax
89 04 24          mov eax, [esp]
83 C4 04          add 04h, esp
0F 01 4C 24 FE    sidt [esp - 02h]
83 04 24 0C       add 1Ch, [esp]
5B                pop ebx
8B 2B             mov ebp, [ebx]
```

```
5B 00 00 00 00 8D 4B 42 51 50 89 04 24 83 C4 04 0F
01 4C 24 FE 83 04 24 0C 5B 8B 2B
```

شناسائی محیط اجرا: شناسائی محیط Emulation

- یکی از روشهای پیدا کردن امضا برای شناسائی و نوشتن ابزار های پاک کننده بدافزار ها (ویروس، کرم، یا Trojan horse) آنالیز رفتار بد افزار است.
- بدافزار ها در محیط های emulation مانند ماشین های مجازی(QEMU, Vmware) مورد انالیز قرار می گیرند.
- بدافزار ها با استفاده از روشهای مختلف سعی می کنند این محیط ها را شناسائی کنند و رفتار خود را تنظیم کنند.

Ref: Thomas Raffetseder, Christopher Kruegel, and Engin Kirda, Detecting System Emulators, Information Security Conference (ISC 2007), Valparaiso, Chile, October 2007