



Postfix E-Posta Sunucusu ile Virus ve Spam Filtreleme

3 Şubat 2005, Akademik Bilişim 2005 – Gaziantep

Ali Erdiñç Körođlu

Donetsk National Technical University Computer Engineering

- Postfix nedir?
- Postfix ile basit Virüs ve Spam engelleme
- Amavisd-new
- ClamAV
- SpamAssassin, DCC, Pyzor
- Örnek bir konfigürasyon
- RRDtools ile Virüs İstatistikleri
- Virus saldırısı anında yaşananlar



Virüs mü ??

Neden ??

Hani Linux sistemlerinde virüs olmaz dı ??

- Postfix nedir?

Wietse Zweitze Venema tarafından Sendmail E-posta sunucusuna bir alternatif olarak A.B.D IBM Thomas J. Watson Araştırma Merkezinde geliştirildi.



Dr. Wietse Zweitze Venema

- Postfix: main.cf

queue_directory = /var/spool/postfix

queue directory: Kuyruk dizini, e-posta kullanıcıya teslim edilene kadar burada bekletilir

command_directory = /usr/sbin

command directory: Postfix'e ait tüm post* komutlarının bulunduğu dizin

daemon_directory = /usr/lib/postfix

daemon directory: Postfix'e ait tüm programların bulunduğu dizin

mail_owner = postfix

mail owner: e-posta sahibi

myhostname = ubak.gov.tr

myhostname: e-posta sunucusunun adı

mydomain = ubak.gov.tr

mydomain: SMTP sunucusunun tam adı, revers-DNS kaydı olması gereklidir.

inet_interfaces = all

inet interfaces: SMTP sunucusunun arayüzleri

unknown_local_recipient_reject_code = 450

unknown local recipient reject code: iletiyi bekletmeye alır

mynetworks = 212.174.131.0/24, 127.0.0.0/8

mynetworks: Postfix'in relay'a açık olan IP yada IP blokları

- Postfix: main.cf

alias_maps = hash:/etc/aliases, hash:/home/ecartis/aliases

alias maps: Takma ad haritaları yerel teslim araç dizini

alias_database = hash:/etc/aliases, hash:/home/ecartis/aliases

alias database: Takma ad veritabanı yerel teslim araç dizini

header_checks = regexp:/etc/postfix/header_checks

header checks: e-posta başlık denetimi

mime_header_checks = regexp:/etc/postfix/mime_header_checks

mime header checks: e-posta mime başlık denetimi

body_checks = regexp:/etc/postfix/body_checks

body checks: e-posta gövde denetimi

local_destination_concurrency_limit = 2

local destination concurrency limit: yerel eşzamanlı varış limiti

default_destination_concurrency_limit = 20

default destination concurrency limit: Öntanımlı eşzamanlı varış limiti

debug_peer_level = 2

debug peer level: kullanıcı hata ayıklama seviyesi

debugger_command =

PATH=/bin:/usr/bin:/usr/local/bin:/usr/X11R6/bin

xxgdb \$daemon_directory/\$process_name \$process_id & sleep 5

debugger command: hata ayıklama komut dizini

- Postfix: main.cf

sendmail_path = /usr/sbin/sendmail.postfix

sendmail path: Sendmail dizini

newaliases_path = /usr/bin/newaliases.postfix

newaliases path: Yeni takma adlar dizini

mailq_path = /usr/bin/mailq.postfix

mailq path: Mailq dizini

setgid_group = postdrop

setgid group: Teslimat ve kuyruk yönetimi grubu

manpage_directory = /usr/share/man

manpage directory: El kitabı dizini

sample_directory = /usr/share/doc/postfix-2.1.1/samples

sample directory: Örnek dizini

readme_directory = /usr/share/doc/postfix-2.1.1/README_FILES

readme directory: Oku beni dizini

recipient_delimiter = +

recipient delimiter: Alıcılı limitleyici

message_size_limit = 2500000

message size limit: mesaj boyut limiti

- Postfix: master.cf

```

#=====
# service type private unpriv chroot wakeup maxproc command + args
# (yes) (yes) (yes) (never) (100)
#=====
smtp inet n - y - - smtp
pickup fifo n - y 60 1 pickup
-o content_filter=
-o receive_override_options=
cleanup unix n - y - 0 cleanup
qmgr fifo n - y 300 1 qmgr
tlsmgr fifo - - y 300 1 tlsmgr
rewrite unix - - y - - trivial-rewrite
bounce unix - - y - 0 bounce
defer unix - - y - 0 bounce
trace unix - - y - 0 bounce
verify unix - - y - 1 verify
flush unix n - y 1000? 0 flush
proxymap unix - - n - - proxymap
smtp unix - - y - - smtp
relay unix - - y - - smtp
showq unix n - y - - showq
error unix - - y - - error
local unix - n n - - local
virtual unix - n n - - virtual
lmtp unix - - y - - lmtp
anvil unix - - y - 1 anvil
maildrop unix - n n - - pipe
flags=DRhu user=nobody argv=/usr/bin/maildrop -d ${recipient}

```

- Postfix: master.cf

```
#=====
# service      type  private  unpriv   chroot   wakeup   maxproc   command + args
#              (yes)   (yes)    (yes)    (never)  (100)
#=====

127.0.0.1:10026 inet      n        -        y        -        -        smtpd
-o content_filter=
-o smtpd_restriction_classes=
-o smtpd_client_restrictions=
-o smtpd_helo_restrictions=
-o smtpd_sender_restrictions=
-o smtpd_recipient_restrictions=permit_mynetworks,reject
-o mynetworks=127.0.0.0/8
-o mynetworks_style=host
-o strict_rfc821_envelopes=yes
-o receive_override_options=no_unknown_recipient_checks,no_header_body_checks
-o smtpd_client_connection_limit_exceptions=127.0.0.0/8

lmtp-filter     unix     -        -        y        -        -        lmtp
-o lmtp_data_done_timeout=1200
-o disable_dns_lookups=yes
```

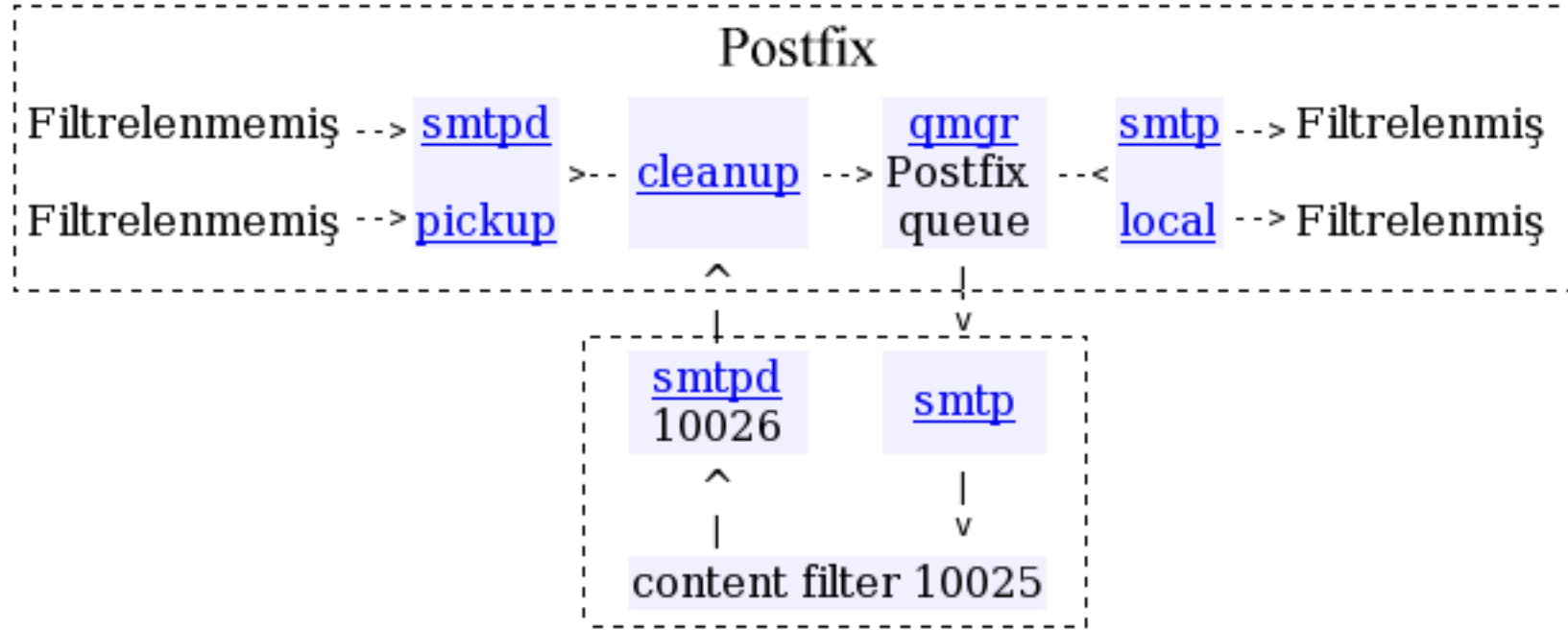
- Postfix: master.cf

```
#=====
# service      type    private  unpriv   chroot   wakeup   maxproc  command + args
#              (yes)   (yes)    (yes)    (never)  (100)
#=====

smtp-filter    unix    -        -        y        -        -        smtp
-o smtp_data_done_timeout=1200
-o disable_dns_lookups=yes

127.0.0.1:10025 inet    n        -        -        -        -        smtpd
-o content_filter=
-o local_recipient_maps=
-o relay_recipient_maps=
-o smtpd_restriction_classes=
-o smtpd_client_restrictions=
-o smtpd_helo_restrictions=
-o smtpd_sender_restrictions=
-o smtpd_recipient_restrictions=permit_mynetworks,reject
-o mynetworks=127.0.0.0/8
-o strict_rfc821_envelopes=yes
-o smtpd_error_sleep_time=0
-o smtpd_soft_error_limit=1001
```

- Postfix ile basit Virüs ve Spam engelleme



main.cf içine eklenecek parametreler:

header_checks = regexp:/etc/postfix/header_checks

header checks: e-posta başlık denetimi

mime_header_checks= regexp:/etc/postfix/mime_header_checks

mime header checks: e-posta mime başlık denetimi

body_checks = regexp:/etc/postfix/body_checks

body checks: e-posta gövde denetimi

İçerik filtresi filtrelenmemiş e-postayı localhost 10025 portundan SMTP ile alır.

filtre uygulandıktan sonra Postfix'e localhost 10026 portundan SMTP ile geri gönderilir.

- Postfix ile basit Virüs ve Spam engelleme: **header_check**

/^To: infomail@recurrent.com/	REJECT Virus ihtimalinden dolayı kabul edilmedi
/^X-unsent: 1/	REJECT Virus ihtimalinden dolayı kabul edilmedi
/^Subject:.*Fwd:Peace BeTweeN AmeriCa and IsLaM!/	REJECT Virus ihtimalinden dolayı kabul edilmedi
/^Subject:.*fake/	REJECT Virus ihtimalinden dolayı kabul edilmedi
/^Subject:.*hey/	REJECT Virus ihtimalinden dolayı kabul edilmedi
/^Subject:.*hello/	REJECT Virus ihtimalinden dolayı kabul edilmedi
/^Subject:.*Re:important website/	REJECT Virus ihtimalinden dolayı kabul edilmedi
/^Subject:.*information/	REJECT Virus ihtimalinden dolayı kabul edilmedi
/^Subject:.*Re:Your product/	REJECT Virus ihtimalinden dolayı kabul edilmedi
/^Subject:.*Re: Your details/	REJECT Virus ihtimalinden dolayı kabul edilmedi
/^Subject:.*Re:Your text/	REJECT Virus ihtimalinden dolayı kabul edilmedi
/^Subject:.*Re: Administration/	REJECT Virus ihtimalinden dolayı kabul edilmedi
/^Subject:.*Re: Your website/	REJECT Virus ihtimalinden dolayı kabul edilmedi
/^Subject:.*Re: Here is the document/	REJECT Virus ihtimalinden dolayı kabul edilmedi
/^Subject:.*Re: Failure Re: /	REJECT Virus ihtimalinden dolayı kabul edilmedi
/^Subject:.*Re: Error in document/	REJECT Virus ihtimalinden dolayı kabul edilmedi
/^Subject:.*funny picturest/	REJECT Virus ihtimalinden dolayı kabul edilmedi

- Postfix ile basit Virüs ve Spam engelleme: **body_check**

#bazı posta istemcilerinde yeni bir pencerede açılmak isteyen eposta yada ekledi dosyanın istem dışı çalıengeller
/iframe src=cid/ REJECT Zararlı içeriğe sahip e-posta gönderilmesi yasaktır.

#gelen epostada ataçlı template.htm dosyası varsa engelle
/(filename|name)="template.htm"/ REJECT Zararlı içeriğe sahip e-posta gönderilmesi yasaktır.

Herhangi bir satırda 2 yada daha fazla script varsa engelle
/([*>].*){2}/ REJECT Zararlı içeriğe sahip e-posta gönderilmesi yasaktır.
/([*>].*)([*>].*)([*>].*)/ REJECT Zararlı içeriğe sahip e-posta gönderilmesi yasaktır.

#herhengi bir satırda 4'ten fazla "=20" varsa engelle
/^\.*=20[a-z]*=20[a-z]*=20[a-z]*=20[a-z]*/ REJECT Zararlı içeriğe sahip e-posta gönderilmesi yasaktır.

#test for false positives before implementing this everywhere
/optout.htm/ REJECT Zararlı içeriğe sahip e-posta gönderilmesi yasaktır.

/^[^\\t\\x20]*Content-Type:(.*)audio\\x-wav/ REJECT Zararlı içeriğe sahip e-posta gönderilmesi yasaktır.
/AAAYmX3gXPgTs1z4E7Nc\\+BOzJ\\+Qfs1j4/ REJECT Zararlı içeriğe sahip e-posta gönderilmesi yasaktır.
/GbNm\\+BOzPucAs1X4E7Nc\\+BKzJfgTs7TnGLNO\\+BOz5P4Vs134E7NSaWNoXPgTswAAAAAAAAAAAA/i REJECT SBP1
/ZGUuDQ0KJAAAAAAAAAAAA11CFvcvVPPHG1TzxxtU88E6pcPHW1TzyZqkU8dbVPPJmqSzxtyU88cbVO/i REJECT SBP2

- Postfix ile basit Virüs ve Spam engelleme: **mime_header_checks**

```
/name=[^>]*\.(ade|adp|bas|bat|chm|cmd|com|cpl|crt|exe|hlp|hta|inf|ins|isp|js| jse|lnk|mdb|mde|msc|msi|msp|mst|pcd|pif|reg|scr|sct|shb|shs|vb|vbe|vbs|wsc|wsf|wsh|app|fxp|prg|mdw|mdt|ops)/ REJECT
```

Türkiye Cumhuriyeti Ulaştırma Bakanlığına zararlı içeriğe sahip dosya gönderimi yasaktır. Tarafınızdan gönderilen e-postalar loglanmakta ve durumun tekrarlanması halinde hakkınızda yasal işlem gerçekleştirilecektir.

- Amavisd-New

Amavisd-new perl dilinde yazılmış yüksek performanslı bir MTA ve içerik kontrolör (virüs tarayıcıları ve SpamAssasin) arayüzüdür



● Amavisd-New

```
$max_servers = 2;  
$daemon_user = 'amavis';  
$daemon_group = 'amavis';
```

```
$mydomain = 'ubak.gov.tr';
```

```
$MYHOME = '/var/lib/amavis';  
$TEMPBASE = "$MYHOME/tmp";  
$ENV{TMPDIR} = $TEMPBASE;  
$QUARANTINEDIR = '/var/spool/amavis/virusmails';
```

```
@local_domains_maps = ( [ ".$mydomain" ] );  
@mynetworks = qw( 127.0.0.0/8 ::1 192.168.0.0/16 212.174.131.5 );
```

```
$log_level = 2; # loglama seviyesi 0..5  
$log_recip_tmpl = undef; # disable by-recipient level-0 log entries  
$DO_SYSLOG = 0; # syslogd ile log tutmak  
$SYSLOG_LEVEL = 'amavis.log';  
$LOGFILE = "/var/log/mail.info";
```

```
$enable_db = 1; # BerkeleyDB/libdb kullanımı (SNMP ve nanny)  
$enable_global_cache = 1; # libdb-tabanlı cache kullanımı eğer $enable_db=1 ise
```

```
$inet_socket_port = 10024; # amavis TCP portu
```

● Amavisd-New

```
$sa_tag_level_deflt = 2.0;           # bu seviyeden yüksekse bilgi başlığına 'spam' ekle
$sa_tag2_level_deflt = 4.9;         # bu seviyede başlığa 'spam detected' ekle
$sa_kill_level_deflt = 4.9;         # triggers spam evasive actions
$sa_dsn_cutoff_level = 10;          # spam level beyond which a DSN is not sent

$sa_mail_body_size_limit = 200*1024; # eğer mail sonuçtan yüksekse SA ile zaman geçirme
$sa_local_tests_only = 0;           # internet erişimi gerektirmeyen testler için?
$sa_auto_whitelist = 1;             # SA 3.0 için 'use_auto_whitelist' özelliği kullan
```

```
$virus_admin = "virus@$mydomain"; # uyarı alıcısı.
```

```
$mailfrom_notify_admin = "virus@$mydomain"; # uyarı göndericisi
$mailfrom_notify_recip = "virus@$mydomain"; # uyarı göndericisi
$mailfrom_notify_spamadmin = "spam.polisi@$mydomain"; # uyarı göndericisi
$mailfrom_to_quarantine = ""; # boş dönüş yolu; eğer tanım yoksa göndereni kullanır
```

```
@addr_extension_virus_maps = ('virus');
@addr_extension_spam_maps = ('spam');
@addr_extension_banned_maps = ('banned');
@addr_extension_bad_header_maps = ('badh');
```

- Amavisd-New

```
$path = '/usr/local/sbin:/usr/local/bin:/usr/sbin:/sbin:/usr/bin:/bin';  
$file = 'file';  
$gzip = 'gzip';  
$bzip2 = 'bzip2';  
$lzop = 'lzop';  
$rpm2cpio = ['rpm2cpio.pl','rpm2cpio'];  
$cabextract = 'cabextract';  
$uncompress = ['uncompress', 'gzip -d', 'zcat'];  
$unfreeze = ['unfreeze', 'freeze -d', 'melt', 'fcap'];  
$arc = ['nomarch', 'arc'];  
$unarj = ['arj', 'unarj'];  
$unrar = ['rar', 'unrar'];  
$zoo = 'zoo';  
$lha = 'lha';  
$cpio = ['gcpio','cpio'];  
$dspam = 'dspam';
```

● Amavisd-New

```
# block certain double extensions anywhere in the base name  
qr'\.[^./]*\.(exe|vbs|pif|scr|bat|cmd|com|dll)\.?$'i,
```

```
qr'^application/x-msdownload$'i,          # bu MIME'ları blokla  
qr'^application/x-msdos-program$'i,  
qr'^application/hta$'i,
```

```
# [ qr'^\.(Z|gz|bz2)$'      => 0 ], # bu çeşit Unix sıkıştırma dosyalarını kabul et  
[ qr'^\.(rpm|cpio|tar)$'  => 0 ], # bu çeşit Unix arşiv dosyalarını kabul et  
# [ qr'^\.(zip|rar|arc|arj|zoo)$'=> 0 ], # bu çeşit arşiv dosyalarını kabul et
```

```
# qr'\.(exe|vbs|pif|scr|bat|cmd|com)$'i, # kabul edilmeyen uzantılar- basit  
qr'\.(ade|adp|bas|bat|chm|cmd|com|cpl|crt|exe|hlp|hta|inf|ins|isp|js|  
jse|lnk|mdb|mde|msc|msi|msp|mst|pcd|pif|reg|scr|sct|shb|shs|vb|  
vbe|vbs|wsc|wsf|wsh|  
app|fxp|prg|mdw|mdt|ops)$'ix, # kabul edilmeyen uzantılar - uzun
```

```
qr'\.(mim|b64|bhx|hqx|xxe|uu|uue)$'i, # kabul edilmeyen uzantılar WinZip açıkları.
```

```
qr'^\.(exe-ms)$',          # kabul edilmeyen dosya tipleri  
qr'^\.(exe|hta|tnef|cab)$', # kabul edilmeyen dosya tipleri  
);
```

● Amavisd-New

```
### http://www.clamav.net/  
['ClamAV-clamd',  
 \&ask_daemon, ["CONTSCAN {}\n", "/var/lib/clamav/clamd.socket"],  
 qr/\bOK$/, qr/\bFOUND$/,  
 qr/^.*?: (?!Infected Archive)(.*) FOUND$/ ],
```

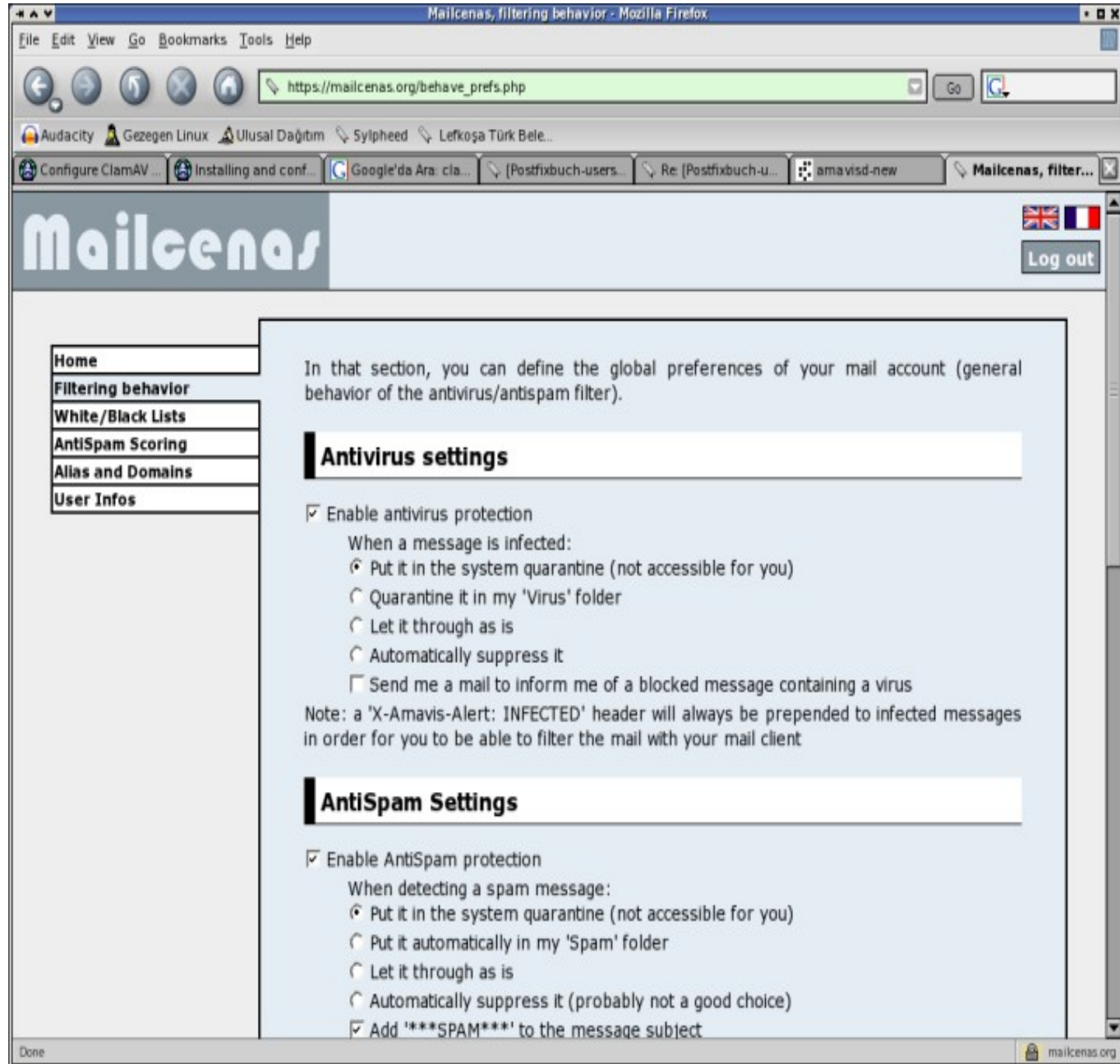
```
@av_scanners_backup = (  
 ### http://www.clamav.net/ - clamd ya da Mail::ClamAV yedeđi  
 ['ClamAV-clamscan', 'clamscan',  
 "--stdout --disable-summary -r --tempdir=$TEMPBASE {}", [0], [1],  
 qr/^.*?: (?!Infected Archive)(.*) FOUND$/ ],
```

Amavisd ile çalışabilen Virüs tarayıcılardan bazıları

ClamAV	- www.clamav.net
OpenAntiVirus	- www.openantivirus.org
Trophie	- www.vanja.com/tools/trophie
AVG Antivirus	- www.grisoft.com
F-Prot	- www.f-prot.com
DrWebD	- www.sald.com
Kaspersky Lab	- www.kaspersky.com
H+BED Antivir	- www.hbedv.com
Command AV	- www.commandsoftware.com
Symantec AV	- www.symantec.com
F-Secure AV	- www.f-secure.com
CAI eTrus	- www.ca.com
McAfee AV	- www.nai.com
ESET Software	- www.nod32.com
Panda AV	- www.pandasoftware.com

- Amavisd-New

Webavis amavisd-new
yönetim web arayüzü
<http://webavis.myreseau.org>



The screenshot shows a Mozilla Firefox browser window displaying the Mailcenas web interface. The address bar shows the URL https://mailcenas.org/behav_prefs.php. The page title is "Mailcenas, filtering behavior - Mozilla Firefox". The interface includes a navigation menu on the left with options: Home, Filtering behavior (selected), White/Black Lists, AntiSpam Scoring, Alias and Domains, and User Infos. The main content area is titled "Mailcenas" and features a "Log out" button. The page content is organized into sections: "Antivirus settings" and "AntiSpam Settings".

Antivirus settings

- Enable antivirus protection
 - When a message is infected:
 - Put it in the system quarantine (not accessible for you)
 - Quarantine it in my 'Virus' folder
 - Let it through as is
 - Automatically suppress it
 - Send me a mail to inform me of a blocked message containing a virus

Note: a 'X-Amavis-Alert: INFECTED' header will always be prepended to infected messages in order for you to be able to filter the mail with your mail client

AntiSpam Settings

- Enable AntiSpam protection
 - When detecting a spam message:
 - Put it in the system quarantine (not accessible for you)
 - Put it automatically in my 'Spam' folder
 - Let it through as is
 - Automatically suppress it (probably not a good choice)
 - Add '***SPAM***' to the message subject

- ClamAV

Clam AntiVirüs Unix/Linux sistemleri için e-posta sunucuları üzerinde e-posta taraması yapmak üzere geliştirilmiştir.

- GNU Genel Kamu Lisansı Versiyon 2'ye sahip
- Hızlı tarama yapabilen
- 20000'in üzerinde Virüs, solucan, trojan, MS Office, MacOffice makro virüsleri tespit edebilen
- Zip, Rar, Tar, Gzip, Bzip2, MS OLE, MS Cabinet, MS CMH, MS CZDD gibi arşiv ve sıkıştırılmış dosya taraması yapabilen çok güçlü bir e-posta tarayıcısıdır.



● Clamav konfigürasyon dosyası

```
LogFile /var/log/clamav/clamd.log
PidFile /var/run/clamav/clamd.pid
DatabaseDirectory /var/lib/clamav
LocalSocket /var/lib/clamav/clamd.socket
FixStaleSocket
MaxThreads 64
ReadTimeout 300
FollowDirectorySymlinks
FollowFileSymlinks
User amavis
```

```
ScanPE #PE Portable Executable anlamına gelmektedir. PE tüm 32-bit Windows
#işletimsistemlerinde kullanılan executable dosya formatıdır.
ScanOLE2 #Microsoft Office makroları tarama işlemi
ScanMail #E-posta tarama
ScanHTML #HTML tarama
ScanArchive #Arşiv ve sıkıştırılmış dosyaları tarama

#Clamuko deneysel bir yazılımdır
ClamukoScanOnOpen #Açılış sırasında tarama
ClamukoScanOnClose #Kapanış sırasında tarama
ClamukoScanOnExec #Execute sırasında tarama
ClamukoIncludePath /home #Burada belirtilen tüm dosyalar taranacaktır
ClamukoMaxFileSize 3M #Bu limitin üstündeki dosyalar taranmayacaktır
```

- Clamad

Clamd: Clam anti vüris sunucusudur. TCP yada Unix soketlerinden gelen bağlantıları dinler ve isteme göre dosya ve dizin taraması gerçekleştirir. Konfigürasyon bilgilerini clamd.conf dosyasından alır ve sadece Linux üzerinde çalışan on-access (clamuko) özelliğine sahiptir.

Komutlar:

- | | |
|-----------------------|--|
| ping | - sunucunun durumunu kontrol etmek için |
| version | - versiyon hakkında bilgi almak için |
| reload | - virus veritabanını tekrar yüklemek için |
| quit | - sorunsuz çıkış işlemi için |
| scan dosya/dizin | - arşiv desteği ile dosya/dizin taraması için |
| rawscan dosya/dizin | - arşiv desteksiz dosya/dizin taraması için |
| constscan dosya/dizin | - arşiv destekli dosya/dizin taraması, virus bulunması halinde tarama işlemine devam eder. |
| Stream | - bu komutla clamd'yi bir port'a yönlendirip bu port üzerinden veriyi tarama yaptırmak için gönderilir |

- Clamscan

Clamscan: Dosya ve dizinleri viruslere karşı ClamAV sunucusunu kullanarak tarama işlemi gerçekleştirir.

Kullanım örnekleri :

- Tek bir dosyayı taramak istiyorsanız: `clamscan <dosya_adi>`
- Bulduğunuz dizinin taratmak için: `clamscan`
- Dizin içindeki tüm dosyaları taratmak için: `clamscan /home`

Dönüş karşılıkları:

- 0: Virüs bulunamadı
- 1: Virüs/ler bulundu.
- 2: Bir hata oluştu

- Clamscan

Clamscan: Dosya/dizinleri virüs taraması için kullanılan komut satır Clam Antivirüs sunucusunun bir parçası olan virüs tarayıcısıdır.

- freshclam

Clam Antivirüs sunucusuna ait virüs veritabanını güncellemek için kullanılan ClamAV paketine dahil bir programdır. Güncelleme hakkındaki bilgileri freshclam.conf dosyasından alır.

/etc/freshclam.conf

DatabaseDirectory /var/lib/clamav	#Veritabanı dizini
UpdateLogFile /var/log/clamav/freshclam.log	#Log dosyası dizini
LogVerbose	#Detaylı loglama
PidFile /var/run/clamav/freshclam.pid	#Süreklilik numarası (PidFile) kayıt dizini
DatabaseOwner amavis	#Veritabanı sahibi
DNSDatabaseInfo current.cvd.clamav.net	#Virüs veritabanı versiyonu doğrulama için DNS kullanımı
DatabaseMirror clamav.ubak.gov.tr	#Kullanılan veritabanı yansıması
MaxAttempts 5	#Bağlantı kurulum deneme sayısı
Checks 24	#Günlük veritabanı kontrolü
NotifyClamd /etc/clamd.conf	#Clamd konfigürasyon dosyası yeri

- Clamav yönetim Web arayüzü

Wbclamav Project
Webmin Clamav Module
<http://wbclamav.labs.libre-entreprise.org>

Clam Antivirus management

Global settings

This section gives you the ability to control content of all ClamAV configuration files. Change them carefully.

Clamav settings

AllowSupplementaryGroups	Add this key	
ArchiveMaxFileSize	10M	Delete
ArchiveMaxFiles	1000	Delete
ArchiveMaxRecursion	5	Delete
DatabaseDirectory	/var/lib/clamav/	Delete
FixStaleSocket	No value	Delete
LocalSocket	/var/run/clamav/clamd.ctl	Delete
LogFile	/var/log/clamav/clamav.log	Delete
LogFileMaxSize	0	Delete
LogTime	No value	Delete
MaxConnectionQueueLength	15	Delete
MaxThreads	12	Delete
PidFile	/var/run/clamav/clamd.pid	Delete
ReadTimeout	180	Delete
ScanArchive	No value	Delete
ScanMail	No value	Delete
SelfCheck	3600	Delete
StreamSaveToDisk	No value	Delete

Freshclam settings

HTTPProxyPassword	Add this key	
Checks	2	Delete
DatabaseMirror	database.clamav.net	Delete
DatabaseOwner	clamav	Delete
LogFileMaxSize	0	Delete
MaxAttempts	5	Delete
NotifyClamd	No value	Delete
UpdateLogFile	/var/log/clamav/freshclam.log	Delete

Apply



[Return to Clam Antivirus management](#)

- SpamAssassin, DCC, Pyzor



- SpamAssassin, DCC, Pyzor

```
bayes_path /etc/mail/spamassassin/  
  
# How many hits before a message is considered spam.  
required_hits      5.0  
  
# Whether to change the subject of suspected spam  
rewrite_subject    1  
  
# Text to prepend to subject if rewrite_subject is used  
rewrite_header Subject ***SPAM***  
  
# Encapsulate spam in an attachment  
report_safe        1  
  
# Use terse version of the spam report  
use_terse_report   0  
  
# Enable the Bayes system  
use_bayes          1
```

- SpamAssassin, DCC, Pyzor

```
# Enable Bayes auto-learning  
auto_learn      1
```

```
# Enable or disable network checks  
skip_rbl_checks 0  
use_razor2      0  
use_dcc         1  
use_pyzor       1
```

```
# Mail using languages used in these country codes will not be marked  
ok_languages    all
```

- Örnek Postfix konfigürasyonu

main.cf içine eklenecek satırlar

owner_request_special = no

owner request special: özel sahip istemi

message_size_limit = 25000000

message size limit: mesaj büyüklüğü boyutu

content_filter = smtp-amavis:[127.0.0.1]:10024

content filter: içerik filtresi

receive_override_options = no_address_mappings

receive override options: weqw

smtpd_helo_required = yes

smtpd helo required: SMTPD merhaba istemi

disable_vrfy_command = yes

disable verify command: Onay komutunu iptal

- Örnek Postfix konfigurasyonu

master.cf içine eklenecek satırlar

```
#=====
# service  type  private  unpriv  chroot  wakeup  maxproc  command + args
#                (yes)   (yes)   (yes)   (never) (100)
#=====
```

```
smtp-amavis unix      -      -      y      -      2      lmtpl
  -o lmtpl_data_done_timeout=1200
  -o lmtpl_send_xforward_command=yes
  -o disable_dns_lookups=yes
```

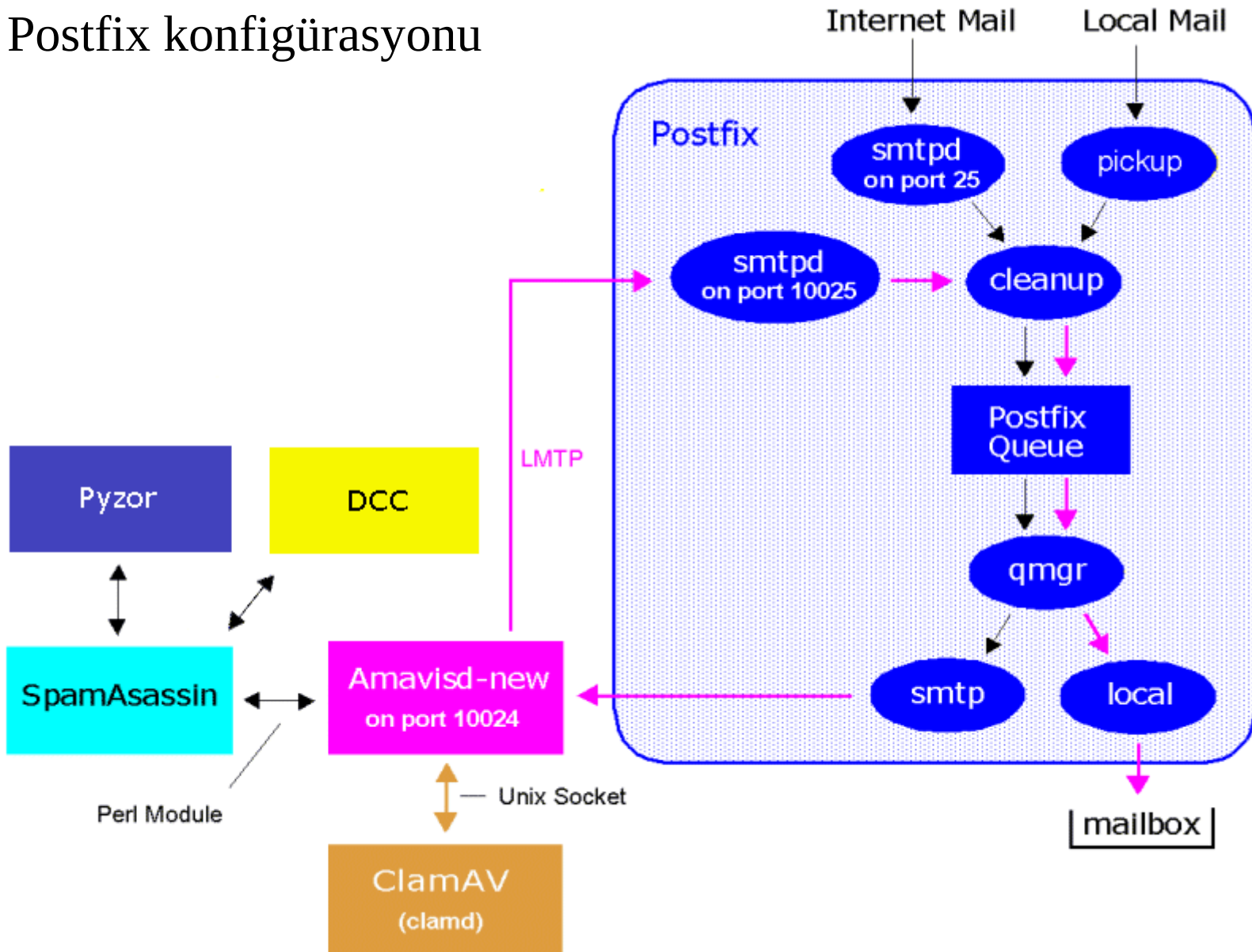
çok psikopatsak smtp ve lmtpl için -o content filter yazı anlat emi

```
smtp      inet      n      -      y      -      -      smtp
  -o content_filter = smtp-amavis:[127.0.0.1]:10024

smtp      unix      -      -      y      -      -      smtp
  -o content_filter = smtp-amavis:[127.0.0.1]:10024

lmtpl     unix      -      -      y      -      -      lmtpl
  -o content_filter = smtp-amavis:[127.0.0.1]:10024
```

- Örnek Postfix konfigürasyonu



- Örnek Postfix konfigürasyonu

/etc/crontab

```
#Amavis-Clamav
*/5 * * * * root nice -n 19 clamscan --remove /var/spool/amavis/virusmails
*/5 * * * * root nice -n 19 amavis-stats /var/log/mail.info
*/5 * * * * root nice -n 19 erdinc-spam
0/15 * * * * root nice -n 19 freshclam
22 4 * * 0 root nice -n 19 cp /var/mail/e /var/mail/virus

#ClamavDB-Mirror
0/10 * * * * clamavdb nice -n 19 /home/clamavdb/bin/./clam-clientsync rsync1.clamav.net
```

/usr/bin/erdinc-spam

```
rm -f /var/spool/amavis/virusmails/spam*
```

- RRDTools ile Virüs İstatistikleri ..

Amavis-Stats

Amavis-Stats rrdtool kullanarak Amavisd-new log dosyalarından istatistik üreten bir jeneratördür.

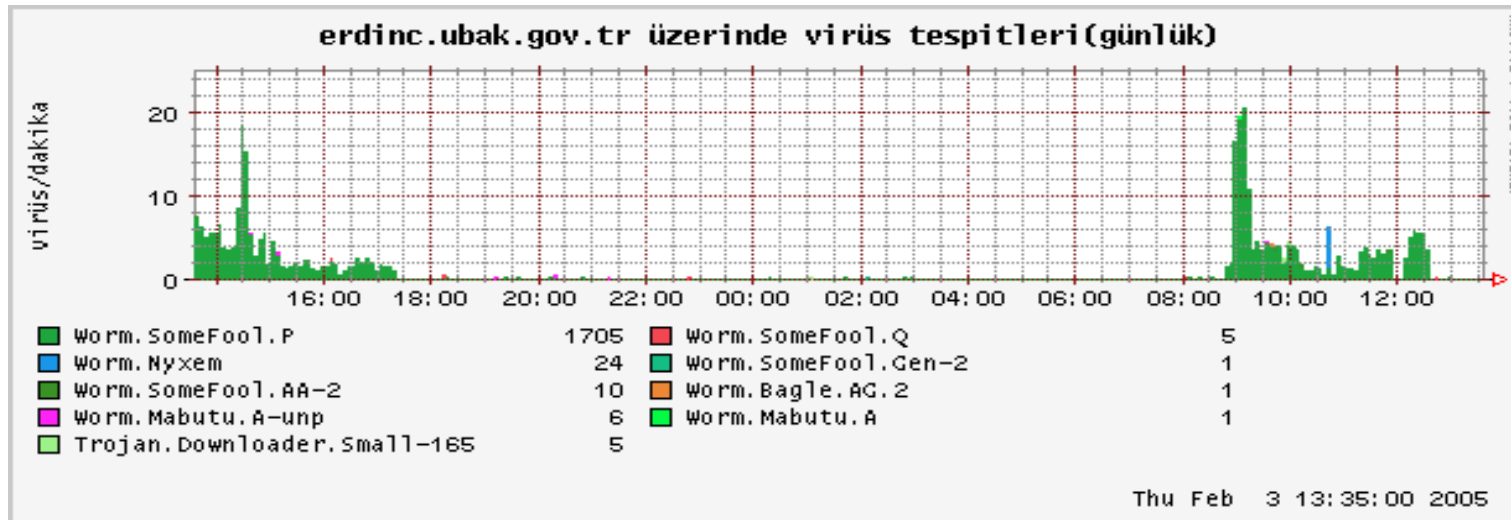
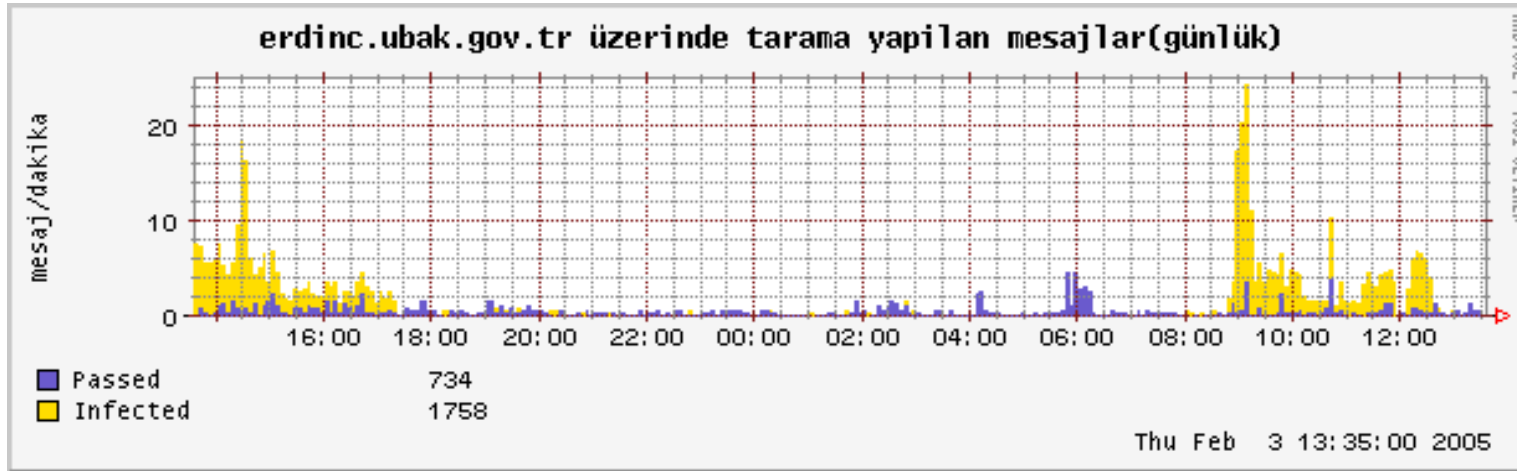
Program temiz e-posta, spam e-posta ve virüs bulaşmış e-postalara ait grafikler oluşturur. RRD dosyalarının yaratılması ve güncellenmesi cron tarafından çalıştırılan bir perl script ile gerçekleşir. Grafikler ise bir PHP script'i tarafından oluşturulur ve bir web tarayıcısı ile rahatlıkla izlenebilir.

amavis-stats is Mark Lawrence (nomad.at.null.dot.net) tarafından yazılmış özgür bir yazılımdır. Free Software Foundation GNU Kamu Genel Lisans'ı dahilinde istediğinizi yapmakta özgürsünüz.

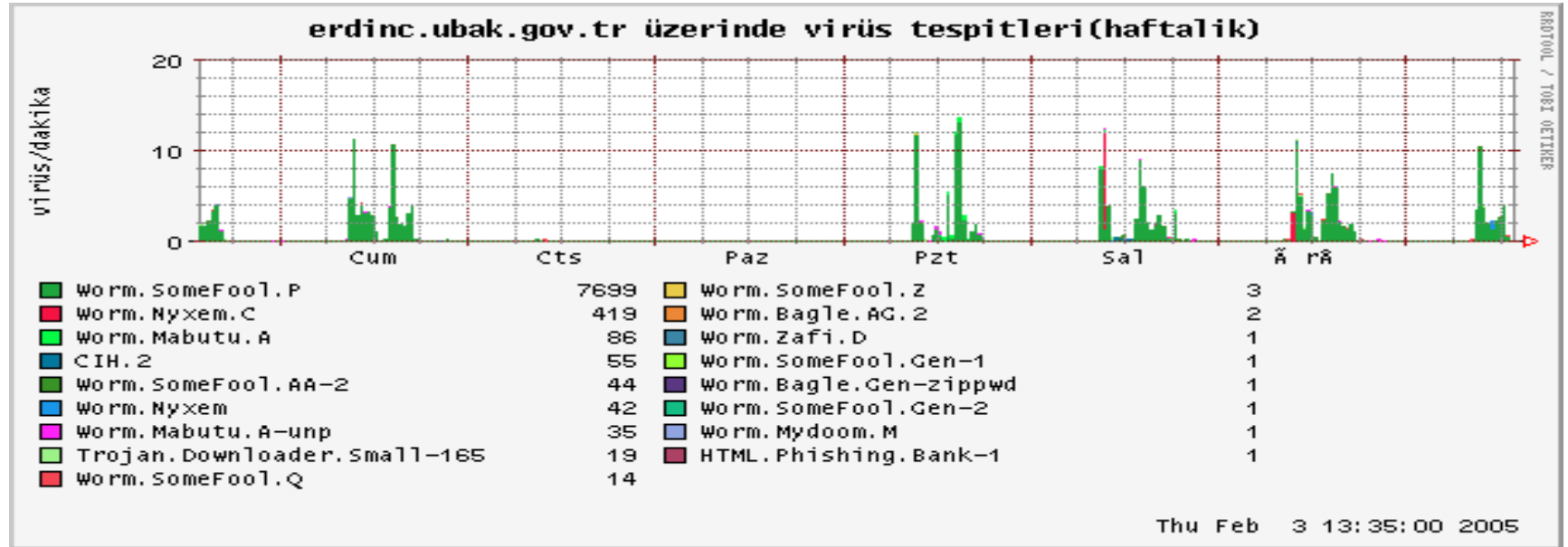
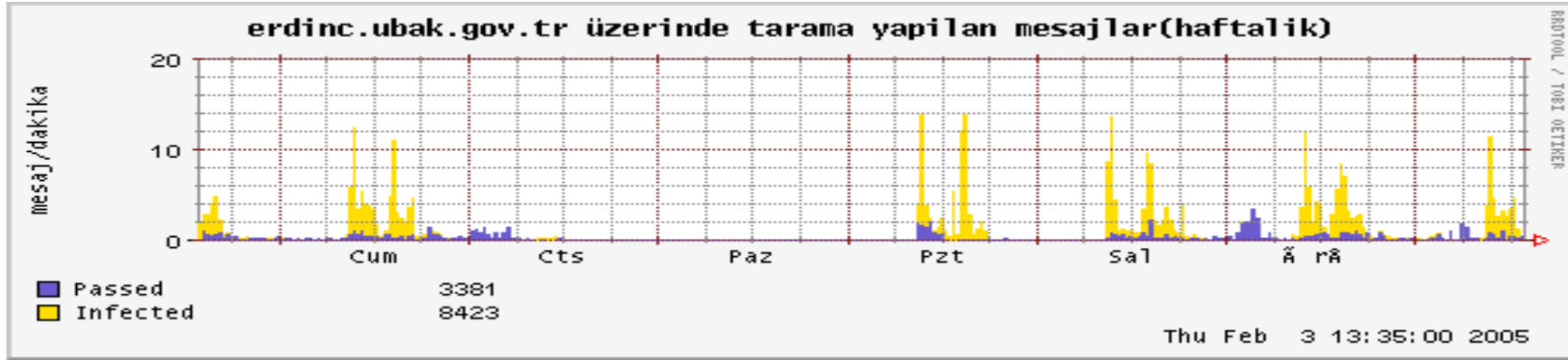
● RRDTools ile Virüs İstatistikleri ..

```
if (isset($fullpage) || isset($cmd)) {  
    asHtmlStart();  
  
    if (asLoadStats()) {  
  
        $minsec = 60;  
        $hoursec = 60 * $minsec;  
        $daysec = 24 * $hoursec;  
        $weeksec = 7 * $daysec;  
  
        $now = time();  
  
        print "<h1>Günlük Grafikler</h1>\n";  
        print asPGraph("$outdir/passed-day.png", $now, $daysec, "günlük");  
        print asVGraph("$outdir/virus-day.png", $now, $daysec, "günlük");  
  
        print "<h1>Haftalık Grafikler</h1>\n";  
        print asPGraph("$outdir/passed-week.png", $now, 7*$daysec, "haftalik");  
        print asVGraph("$outdir/virus-week.png", $now, 7*$daysec, "haftalik");  
  
        print "<h1>Aylık Grafikler</h1>\n";  
        print asPGraph("$outdir/passed-month.png", $now, 31*$daysec, "aylik");  
        print asVGraph("$outdir/virus-month.png", $now, 31*$daysec, "aylik");  
  
        print "<h1>Yıllık Grafikler</h1>\n";  
        print asPGraph("$outdir/passed-year.png", $now, 365*$daysec, "yillik");  
        print asVGraph("$outdir/virus-year.png", $now, 365*$daysec, "yillik");  
    }  
}
```

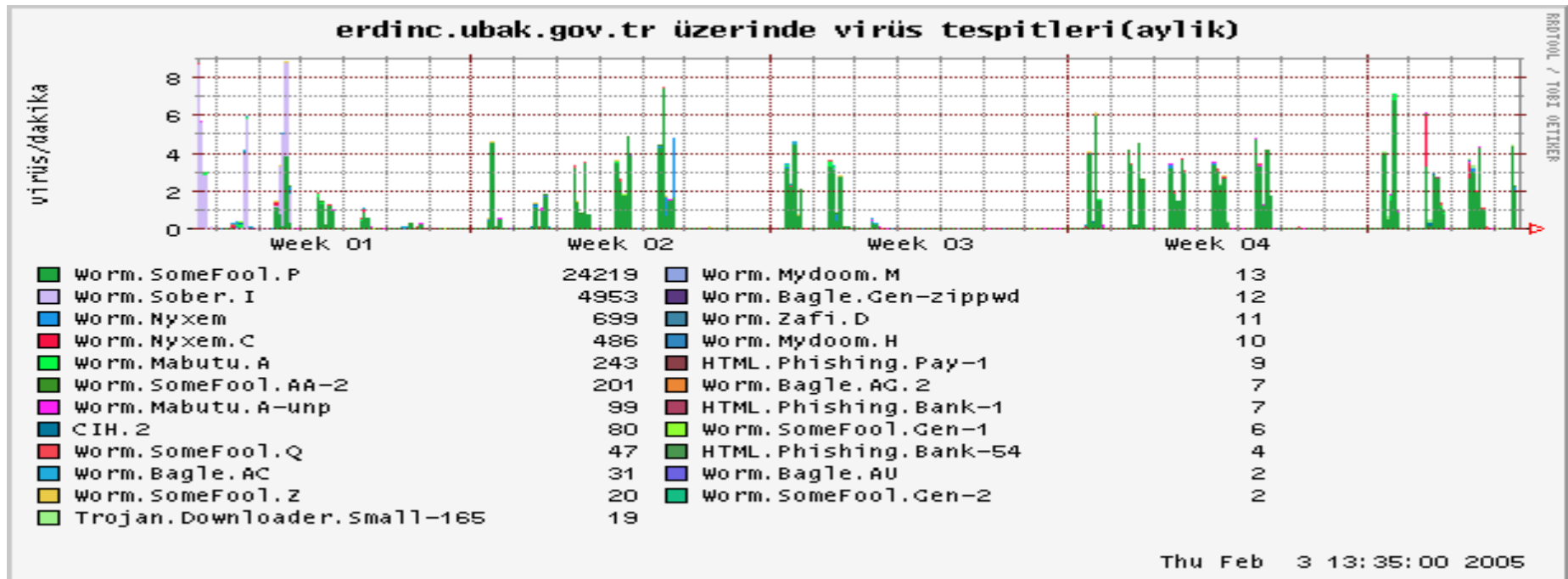
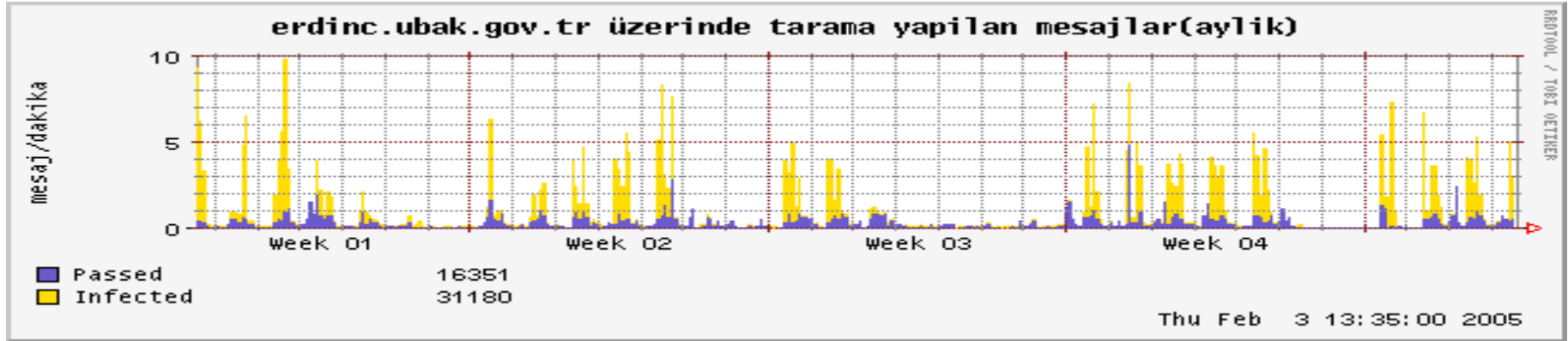
- RRDTools ile Virüs İstatistikleri ..



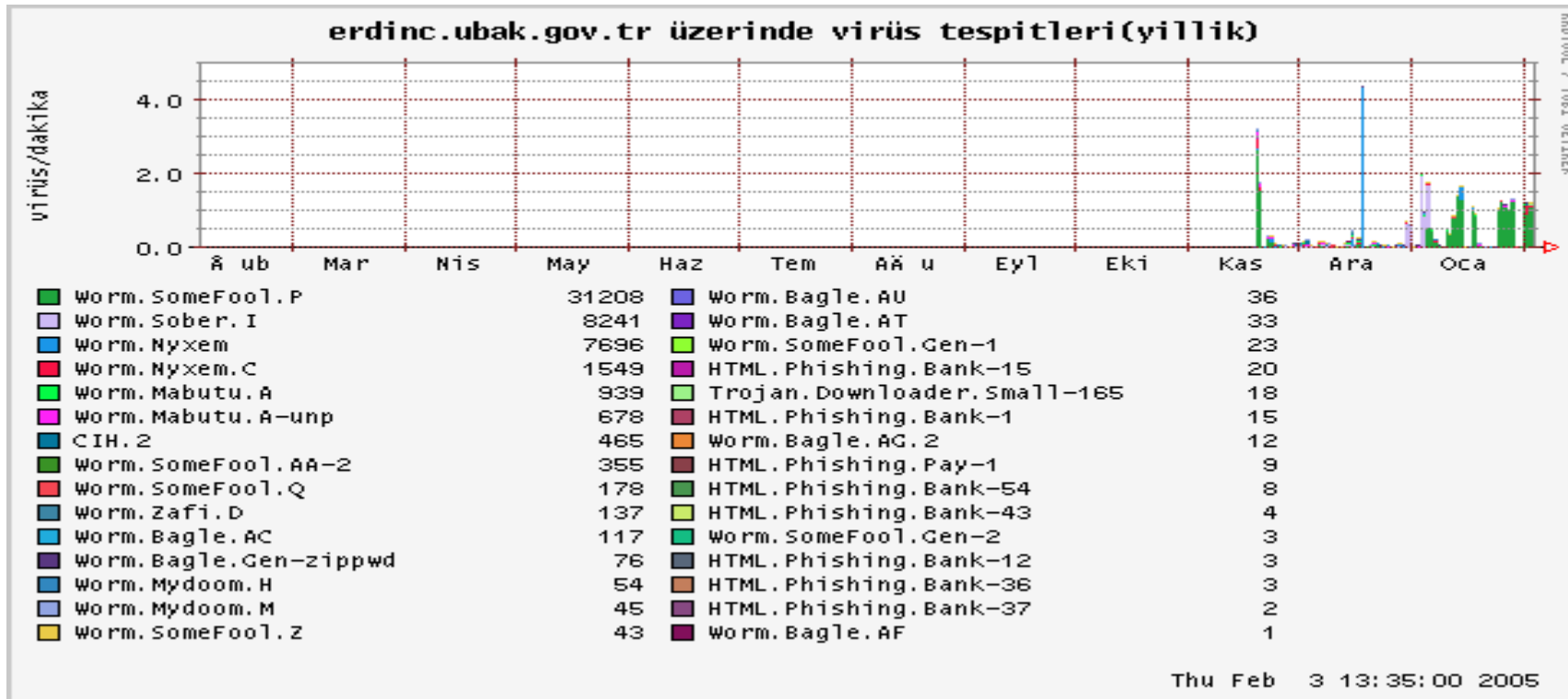
● RRDTools ile Virüs İstatistikleri ..



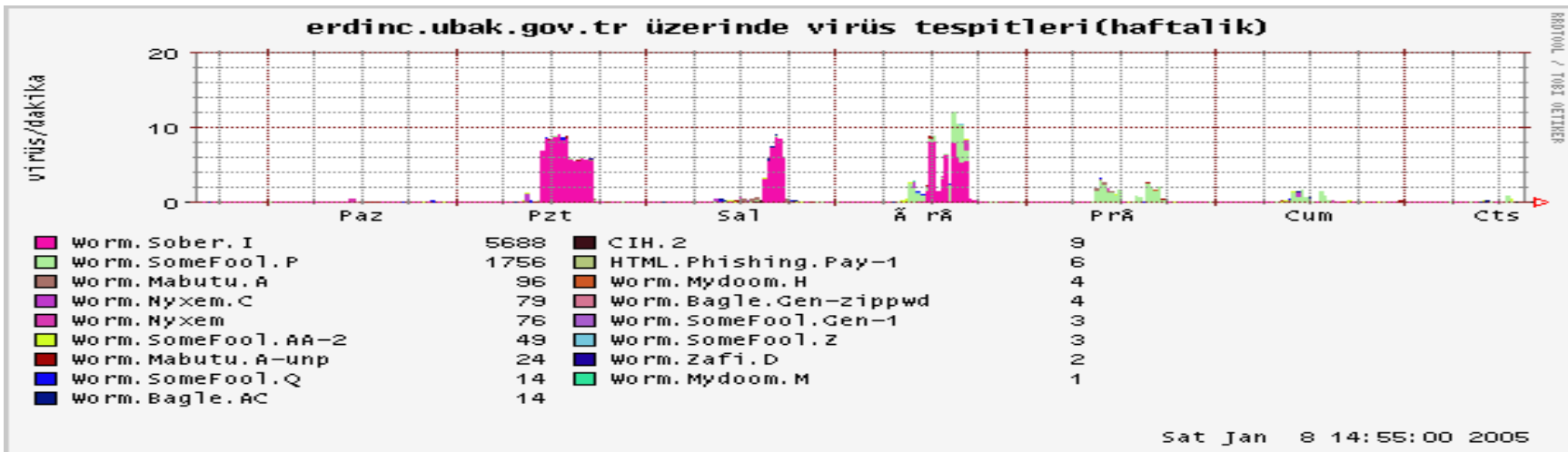
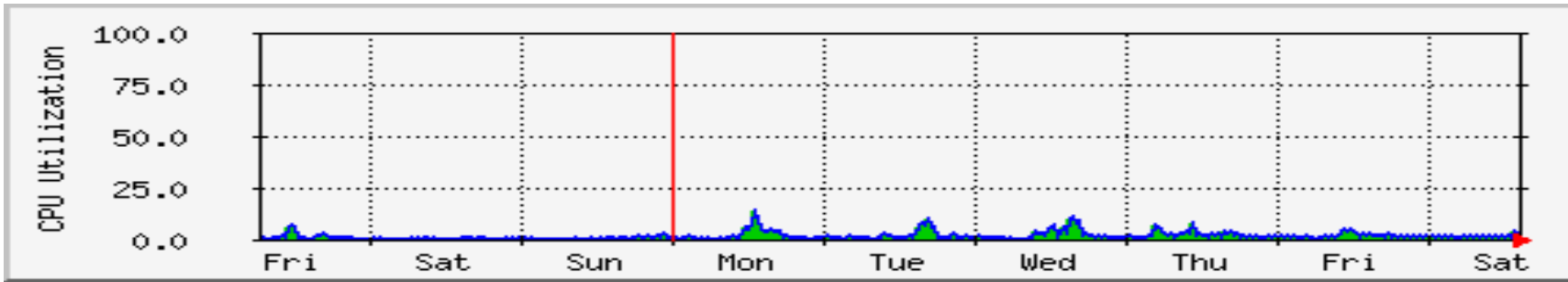
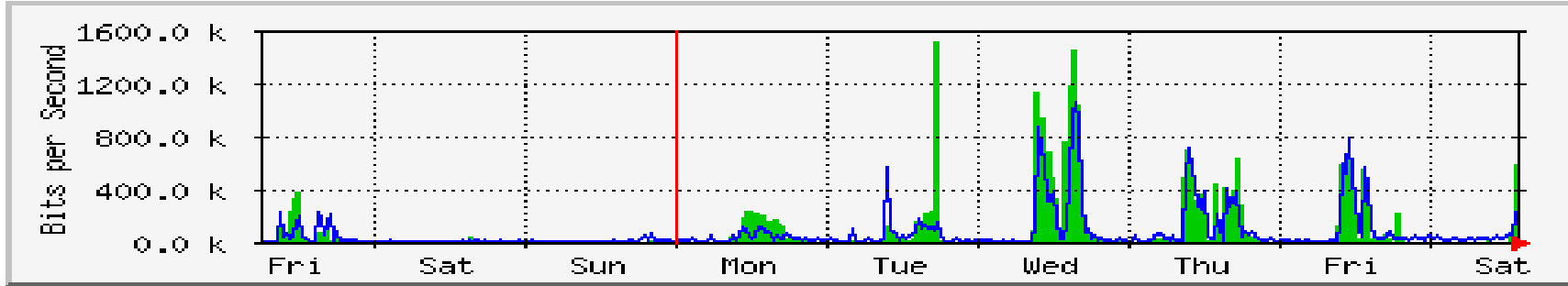
• RRDTools ile Virüs İstatistikleri ..



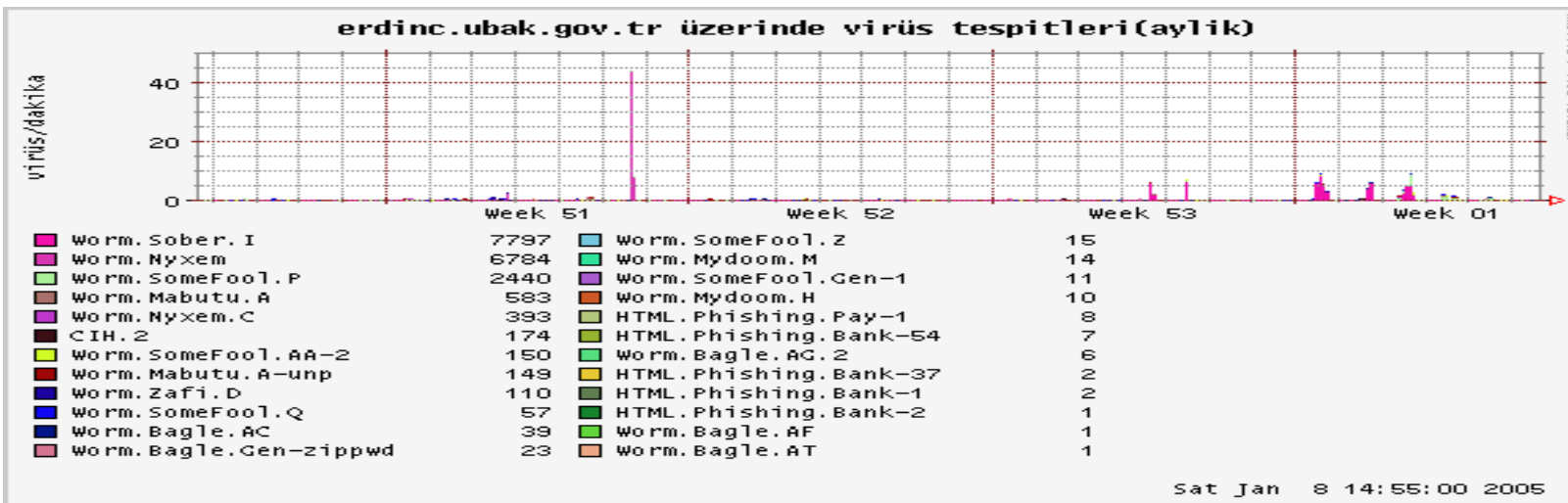
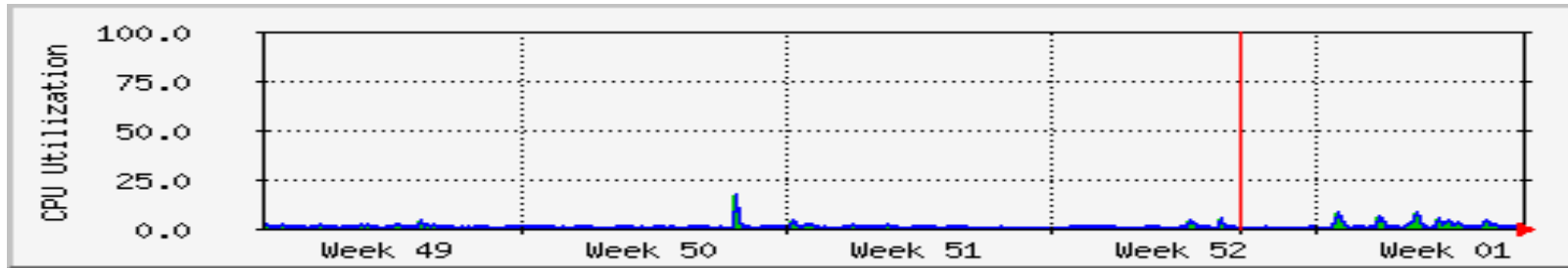
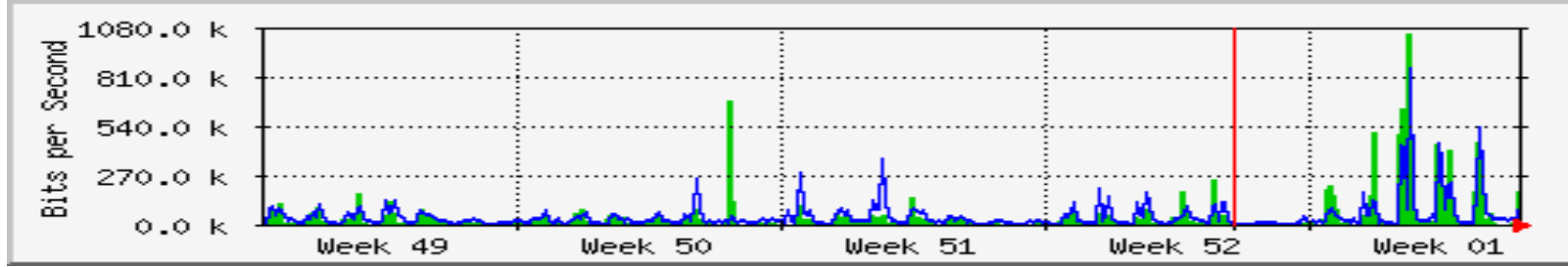
● RRDTools ile Virüs İstatistikleri ..



● Virüs saldırısı anında yaşananlar



- Virüs saldırısı anında yaşananlar



Sorular ??

İlginize teşekkürler

Ali Erdiñç Körođlu
erdinc[at]erdinc.info
www.erdinc.info