

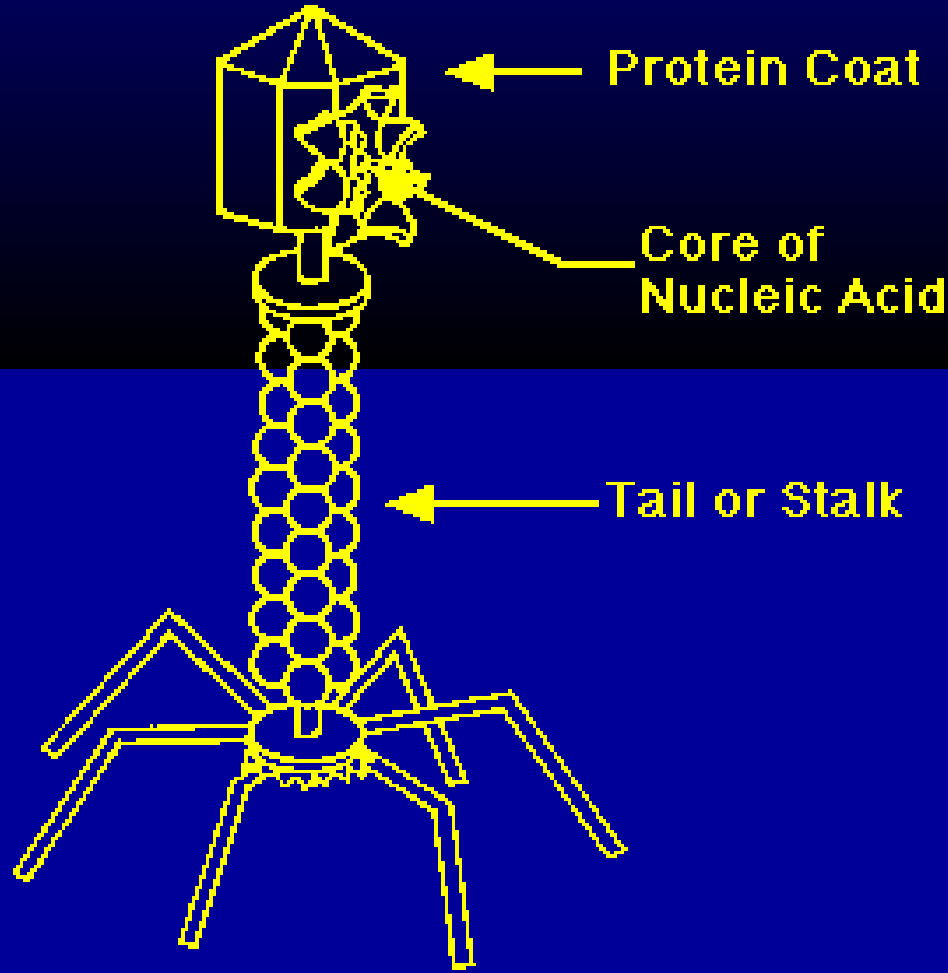
# VIRUS INHIBITION

Sunan:

Serdar KÖYLÜ  
Fişek ENSTİTÜSÜ

# Virüs Nedir ?

---



Virüs terimi,  
Tıp kaynaklarından  
alınmıştır.

Normalde cansız  
oldukları halde,  
Herhangi bir hücre  
içine girdikleri anda  
üreyip, hücrenin  
fonksiyonlarını ele  
geçirebilen  
moleküllerdir.

# Bilgisayar Virüsleri ?

---



**Bilgisayarların bilgiden daha hızlı yayılması nedeniyle,  
Virüs kavramı deforme olmuş;  
Bazı sistem sorumluları  
anlayamadıkları şeylere virüs  
diyerek işin içinden sıyrılmayı  
tercih etmiştir.**

# Bilgisayar Virüsleri ?

---

## **VİRÜS**

Kendini çoğaltabilen,

İstem dışı çalışan,

Kendini gizleyebilen,

**KODLARA VERİLEN  
GENEL İSİMDİR**

Tipik bir virüs saldırısı :))



# Bilgisayar Virüsleri ?

---

## **VİRÜS / SOLUCAN**

Programlara,  
Sistem bölgelerine,  
Firmware (BIOS)'a,

## **VİRÜS**

Tipik bir virüs saldırısı :))



# Bilgisayar Virüsleri ?

---

## **VİRÜS/SOLUCAN**

Tek başına çalışabilen,  
Sistemlerdeki açıkları kullanan,  
Bilhassa ağ üzerinden yayılan,

## **SOLUCAN/WORM**

Tipik bir virüs saldırısı :))



# Virüslerin zararları

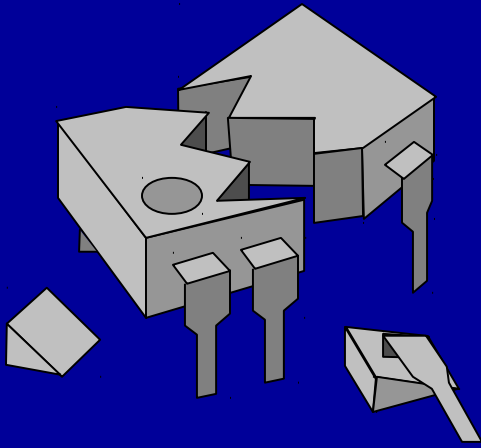
---



Dosya sistemlerini silebilirler (format)

Programları bozabilirler.

Dosyaları silebilirler.



Nadiren donanıma zarar verirler.

FLASH BIOS'ları silmek.

Çok eski monitörlerde V+H sinyalleri ile HV Çıkışlarını yakmak.

# Virüslerin zararları

---



Son dönemde yaygınlaşan solucanların tipik zararları, ağ trafiğini artırmak, serverleri gereksiz meşgul etmek ve en önemlisi bilgileri bilinmeyen makinelere yollamaktır.



# Virüslerin zararları

---

Ticari sırların ele geçmesi tehlikesi

İş gücü kaybı

Temizleme ve korunma maliyetleri

Prestij kaybı....



Global ekonomiye verilen milyarlarca dolarlık zarar

# Virüs Türleri

---

## Bulaşma bölgesine göre virüsler

Boot Virüsleri

Dosya Virüsleri

Makro/Script Virüsleri

Karışık virüsler

Solucanlar

Disketlerin Boot Sektörleri

Harddisklerin MBR Kayıtları

## Bulaşma bölgesine göre virüsler

Boot Virüsleri

Dosya Virüsleri

Makro/Script Virüsleri

Karışık virüsler

Solucanlar

Çalıştırılabilir Dosyalar

\* Binary dosyaların:

Kodları içersine  
Kütüphane dosyalarına  
F/S üzerinden başlatma

# Virüs Türleri

---

## Bulaşma bölgesine göre virüsler

Boot Virüsleri

Dosya Virüsleri

Makro/Script Virüsleri

Karışık virüsler

Solucanlar

Excel/Word vs.

Javascript

BASH, WSH, \*.BAT....

# Virüs Türleri

---

## Bulaşma bölgesine göre virüsler

Boot Virüsleri

Dosya Virüsleri

Makro/Script Virüsleri

Karışık virüsler

Solucanlar

Multi-partiate...

Aynı anda birden çok yere bulaşabilen virüsler.

## Bulaşma bölgesine göre virüsler

Boot Virüsleri

Dosya Virüsleri

Makro/Script Virüsleri

Karışık virüsler

Solucanlar

Herhangi bir yere bulaşmadan kendi başına yaşayabilen virüsler

Yapı olarak diğer virüslere benzer olmakla birlikte yaşamak için başka programlara bağımlılıkları yoktur.

Virüsler nasıl tespit edilebilir ?

---

Genelde verilecek cevap, yanlış olandır:

~~AntiVirüs Kullanın !~~

İstatistik olarak, virüsler ilk ortaya çıktıkları  
dönemde tahribatlarını yaparlar.

Sebebi ise güvendiğiniz programın henüz o virüsü

**TANIYAMAMASIDIR.**

# Virüsler nasıl tespit edilebilir ?

---

## YAPILMASI GEREKENLER

- Sistemdeki virüsten etkilenebilecek noktaları gözetim altında tutmak.
- Ağ üzerindeki anlaşılamayan hareketleri iyi yorumlamak
- Virüslerin sisteme olası etkilerini değerlendirmek
- Virüsler ile ilgili literatürü iyi takip etmek



# Virüslerden etkilenebilecek noktalar..

## NERELER ETKİLENEBİLİR ?

- Teorik olarak, çalışabilir kod içeren, yazılabilir tüm sistem bileşenleri

BIOS & EXT.

Flash ROM Kullanan BIOS'lar.

NVRAM üzerinde kod tutan sistemler.

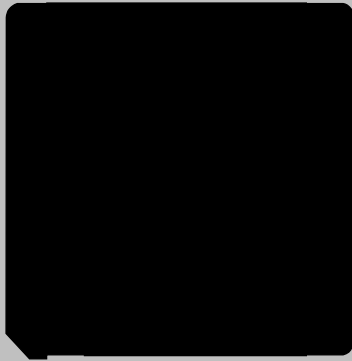


# Virüslerden etkilenebilecek noktalar..

## NERELER ETKİLENEBİLİR ?

- Teorik olarak, çalışabilir kod içeren, yazılabilir tüm sistem bileşenleri

### BOOT BİLEŞENLERİ



**Disketlerin boot sektörleri**

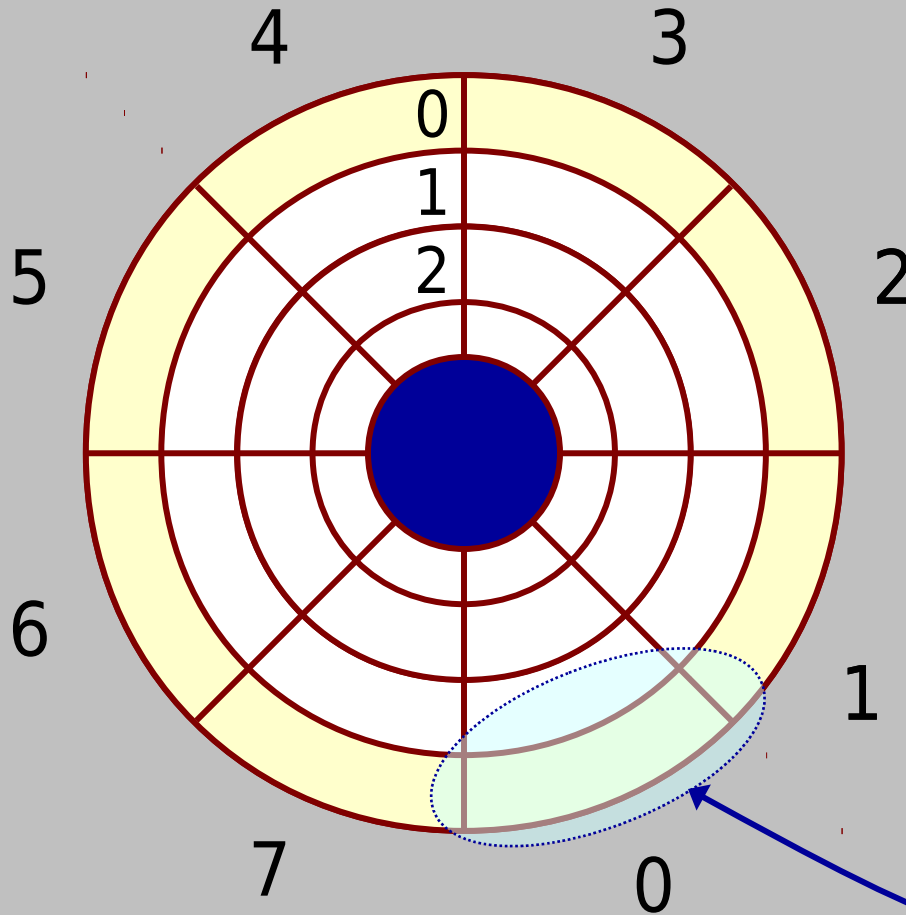


**Harddisk MBR ve BOOT bölümleri**

# Virüslerden etkilenebilecek noktalar..

## NERELER ETKİLENEBİLİR ?

### BOOT BİLEŞENLERİ



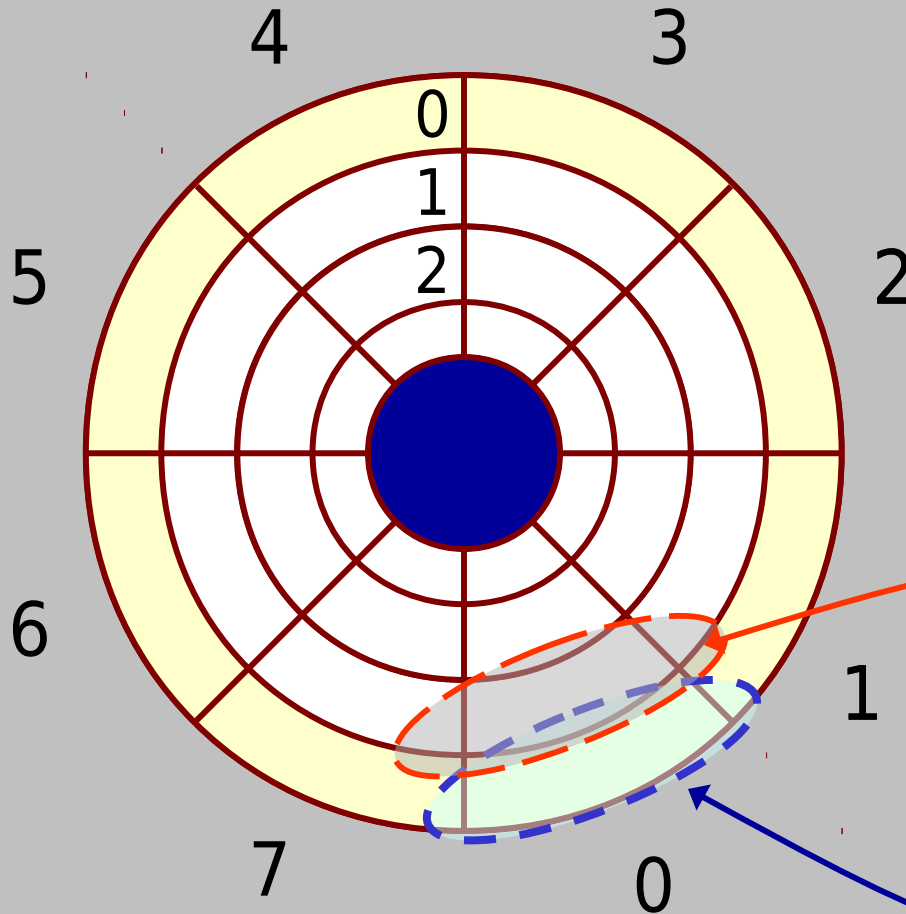
Disketlerin 0 Cyl  
0. Sektörü  
Son 2 Bayt  
0x55AA

**Boot Sektör**

# Virüslerden etkilenebilecek noktalar..

## NERELER ETKİLENEBİLİR ?

### BOOT BİLEŞENLERİ



HD'nin 0 Cyl  
0. Sektörü

Partisyonun  
İlk Sektörü

0x55AA

**BOOT SEKTÖR**

**MBR**

# Virüslerden etkilenebilecek noktalar..

## NERELER ETKİLENEBİLİR ?

- Teorik olarak, çalışabilir kod içeren, yazılabilir tüm sistem bileşenleri

### BOOT BİLEŞENLERİ

X86 PC mimarisinde, BIOS yordamı bu sektörleri kullanarak işletim sistemini yükler. Bu esnada CPU 8086 uyumlu modda çalışır. 640K üzerinde belleğe ulaşamaz.

OS, sistemin düşük değerli adreslerine yerleşir.

# Virüslerden etkilenebilecek noktalar..

---

## NERELER ETKİLENEBİLİR ?

- Teorik olarak, çalışabilir kod içeren, yazılabilir tüm sistem bileşenleri

### BOOT BİLEŞENLERİ

BOOT virüsü, OS'un üzerine yazılmaması için bu belleğin tepesine yerleşir. Bu tür virüslerin aranması gereken yer orasıdır.

9E000 ile 9FFFF arasında kalan bölgeye dikkat edilmelidir.

# Virüslerden etkilenebilecek noktalar..

```
C:\WINDOWS\Desktop>debug
```

```
-a
```

```
0E64:0100 int 13
```

```
0E64:0102
```

```
-t
```

```
AX=0000 BX=0000 CX=0000
```

```
DX=0000
```

```
DS=0E64 ES=0E64 SS=0E64
```

```
CS=FDB2
```

```
FDB2:24CF 63 DB 63
```

```
-t
```

```
AX=0000 BX=0000 CX=0000
```

```
DX=0000
```

```
DS=0E64 ES=0E64 SS=0E64
```

```
CS=035D
```

```
035D:0148 FB STI
```

## TEBİLİR ?

T (Trace) ile, INT 13  
ve INT 21 için  
yaptığınız izleme  
sonucunda

9A00:0000 - 9FFF:0000

Adres bölgesine  
ulaşırsanız, virüs  
bulunması kuvvetle  
muhtemeldir...

# Virüslerden etkilenebilecek noktalar..

## NERELER ETKİLENEBİLİR ?

```
C:\WINDOWS\Desktop>mem
```

Bellek Türü	Toplam	Kullanılan	Boş
-----	-----	--	-----
Geleneksel	640K	31K	609K

```
C:\WINDOWS\Desktop>chkdsk
```

```
....
```

```
....
```

disk üzerinde            75.599 ayırma birimi kullanılabilir

655.360 bayt toplam bellek

623.504 bayt boş



# Virüslerden etkilenebilecek noktalar..

---

## NERELER ETKİLENEBİLİR ?

Kurtulmak için (Windows)

```
A:\>fdisk /mbr
```

```
A:\>C:\WINDOWS\COMMAND\ATTRIB -H -S -R  
C:\MSDOS.SYS
```

```
A:\>COPY C:\MSDOS.SYS C:\MSDOS.OLD
```

```
A:\>sys c:
```

```
A:\>C:\WINDOWS\COMMAND\ATTRIB -H -S -R  
C:\MSDOS.SYS
```

```
A:\>COPY C:\MSDOS.OLD C:\MSDOS.SYS
```

# Virüslerden etkilenebilecek noktalar..

---

## NERELER ETKİLENEBİLİR ?

Kurtulmak için (Linux, sadece MBR)

```
[root@dns /root]# lilo  
Added linux  
Added linux-nonfb *  
Added failsafe  
Added windows  
Added floppy  
[root@dns /root]#
```

# Virüslerden etkilenebilecek noktalar..

## NERELER ETKİLENEBİLİR ?

- Teorik olarak, çalışabilir kod içeren, yazılabilir tüm sistem bileşenleri

### PROGRAMLAR

Programlar ve bunların kullandığı kütüphaneler tehdit altındadır.

DOS COM + EXE Binaryleri, WIN32 PE Binaryleri, Linux ELF ve A.OUT Binaryleri bu tür dosyalardır.

# Virüslerden etkilenebilecek noktalar..

## NERELER ETKİLENEBİLİR ?

### PROGRAMLAR

DOS uzantısı .EXE ve .COM olan dosyaları yürütülebilir dosyalar olarak kabul eder.

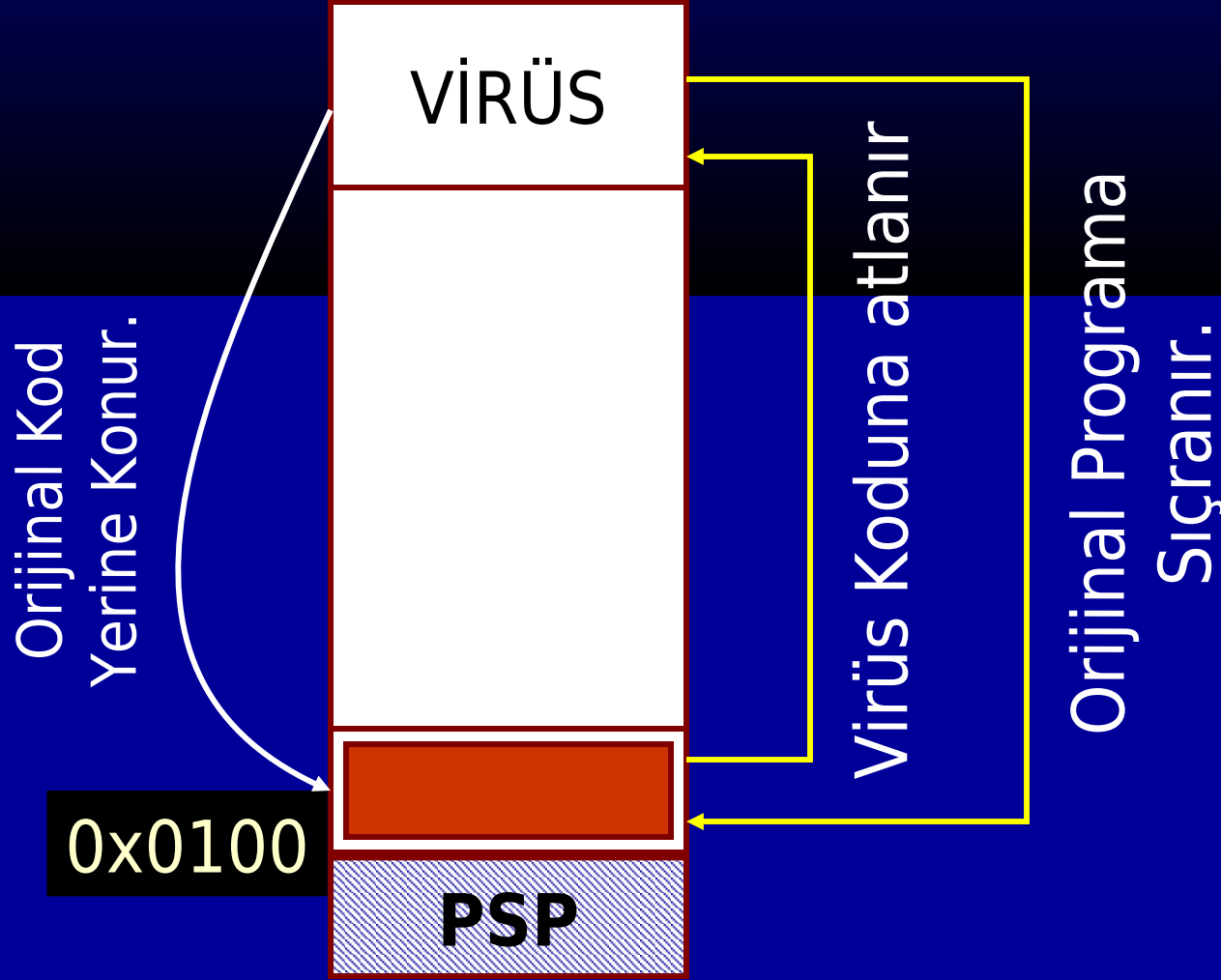
Eğer dosyanın ilk iki baytı MZ ise, bu dosyanın EXE türünde dosya olduğu düşünülür.

Diğer dosyalar için, dosya içeriği belleğe alınır. Yerleşilen segmentin ilk 256 Baytı PSP için ayrılır. 0x0100 adresine yerleşen dosyanın ilk baytına kontrol devredilir.

# Virüslerden etkilenebilecek noktalar..

## NERELER ETKİLENEBİLİR ?

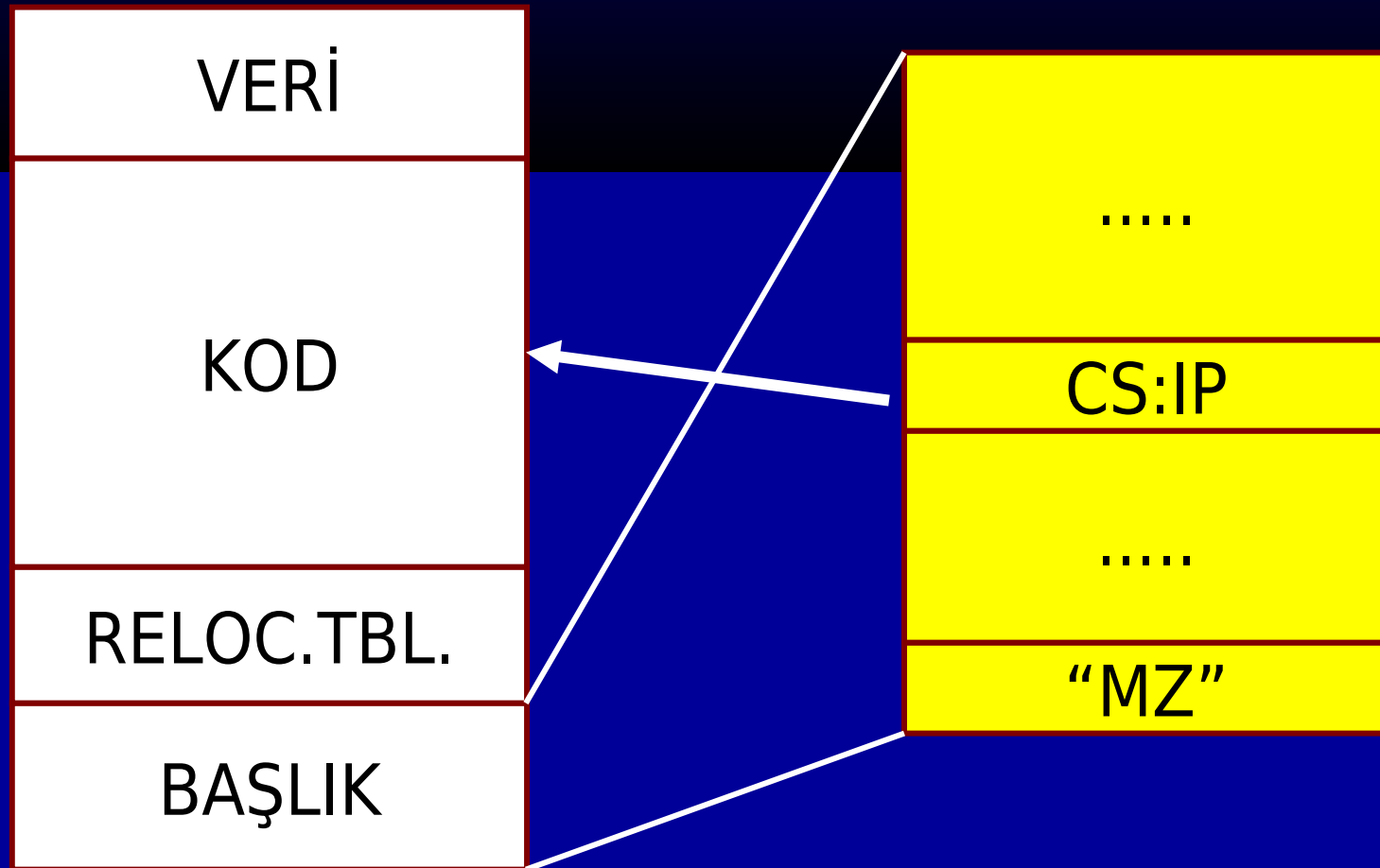
PROGRAMLAR, \*.COM



# Virüslerden etkilenebilecek noktalar..

## NERELER ETKİLENEBİLİR ?

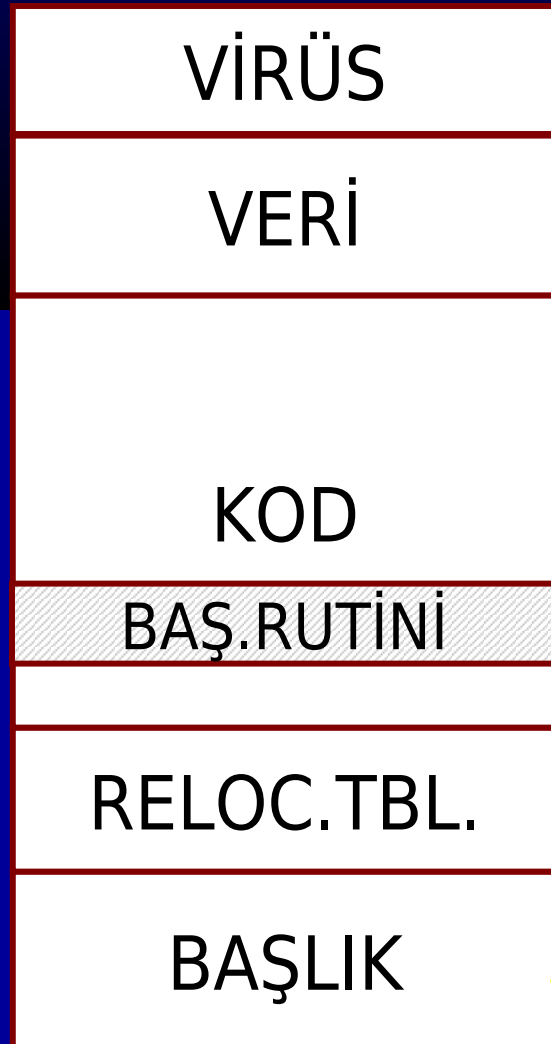
PROGRAMLAR, \*.EXE,DLL VS.



# Virüslerden etkilenebilecek noktalar..

## NERELER ETKİLENEBİLİR ?

PROGRAMLAR, \*.EXE,DLL vs.

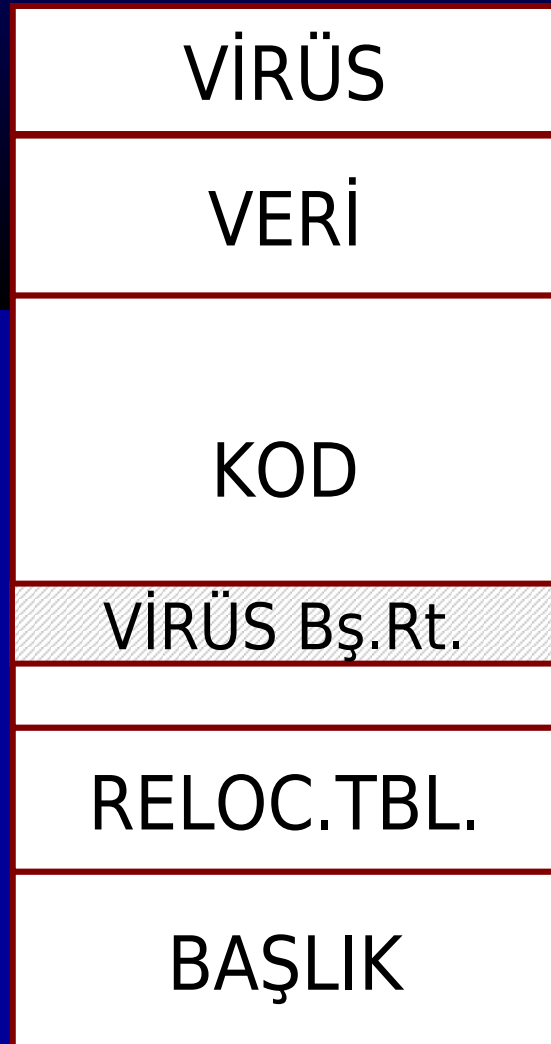


Virüs, Başlıktaki başlangıç adresini kendine çevirebilir.

# Virüslerden etkilenebilecek noktalar..

## NERELER ETKİLENEBİLİR ?

PROGRAMLAR, \*.EXE,DLL vs.



Virüs, Başlangıç rutininin yerine kendi başlangıç rutinini yazabilir.



# Virüslerden etkilenebilecek noktalar..

---

## NERELER ETKİLENEBİLİR ?

PROGRAMLAR, \*.EXE,DLL vs.

Virüslerde, diğer programlar gibi buglara sahiptir.

EXE dosya formatı, sayfalar şeklinde düzenlenir. Ayrıca linker overlay işlemleri için özel sayfalama metotları kullanır.

Sonuçta virüs bulaşmasıyla bu dosyalarda bazı deformasyonlar oluşabilir.

# Virüslerden etkilenebilecek noktalar..

---

## NERELER ETKİLENEBİLİR ?

PROGRAMLAR, \*.EXE,DLL vs.

Sonuçta olmadık yere dosyaların çalışmaması virüs enfeksiyonu olduğuna dair iyi bir ipucudur.

Ayrıca programların çalışırken bilhassa yeni bölümlerde arıza yapması aynı şekilde değerlendirilebilir.

Bozucu etki virüs temizliğinden sonra da görülebilir. Bu durumda çalışabilir dosyaları yedeklerinden geri yüklemek gerekir.

# Virüslerden etkilenebilecek noktalar..

---

## NERELER ETKİLENEBİLİR ?

Programların boyutlarının büyümesi.

Programların belli bir noktasında veya programı çalıştırırken yaşanan sistem sorunları.

Programların açılışında yaşanan yavaşlık.

# Virüslerden etkilenebilecek noktalar..

---

Sahte bir EXE dosyası oluşturun.

1 - 2 Baytlar 'MZ'

6 - 7 Baytlar RELOC Büyüklüğü. = 0

8 - 9 Başlık büyüklüğü. = 32

20 - 21 IP = 0

22 - 23 CS = 0

# Virüslerden etkilenebilecek noktalar..

Sahte bir EXE dosyası oluşturun.

```
\WINDOWS\Desktop>debug
```

```
E64:0100 db 'MZ'  
E64:0102 db 0,0,0,0,0,0  
E64:0108 dw 20  
E64:010A db 0,0,0,0,0,0,0,0,0,0  
E64:0114 dw 0  
E64:0116 dw 0  
E64:0118 db 0,0,0,0,0,0,0,0,0,0  
E64:0122
```

```
-n tuzak.hdr
```

```
-rcx
```

```
CX 0000
```

```
:22
```

```
-w
```

```
00022 bayt yazılıyor
```

```
-q
```

TUZAK.HDR Başlık için gereken dosya.

# Virüslerden etkilenebilecek noktalar..

---

**Sahte bir EXE dosyası oluşturun.**

```
C:\WINDOWS\Desktop>debug
```

```
-a
```

```
0E64:0100 dw 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
```

```
0E64:0120 dw 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
```

```
0E64:0140 dw 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
```

```
0E64:0160
```

```
-n tuzak.bd
```

```
-rcx
```

```
:60
```

```
-w
```

```
-q
```

**TUZAK.BD = Gövdeyi oluşturacak NULL String.**

# Virüslerden etkilenebilecek noktalar..

---

Sahte bir EXE dosyası oluşturun.

```
WINDOWS\Desktop>copy con ct.bat  
TUZAK.BD/b+TUZAK.BD/b TUZAK.BDF  
TUZAK.BDF/b+TUZAK.BDF/b TUZAK.BD
```

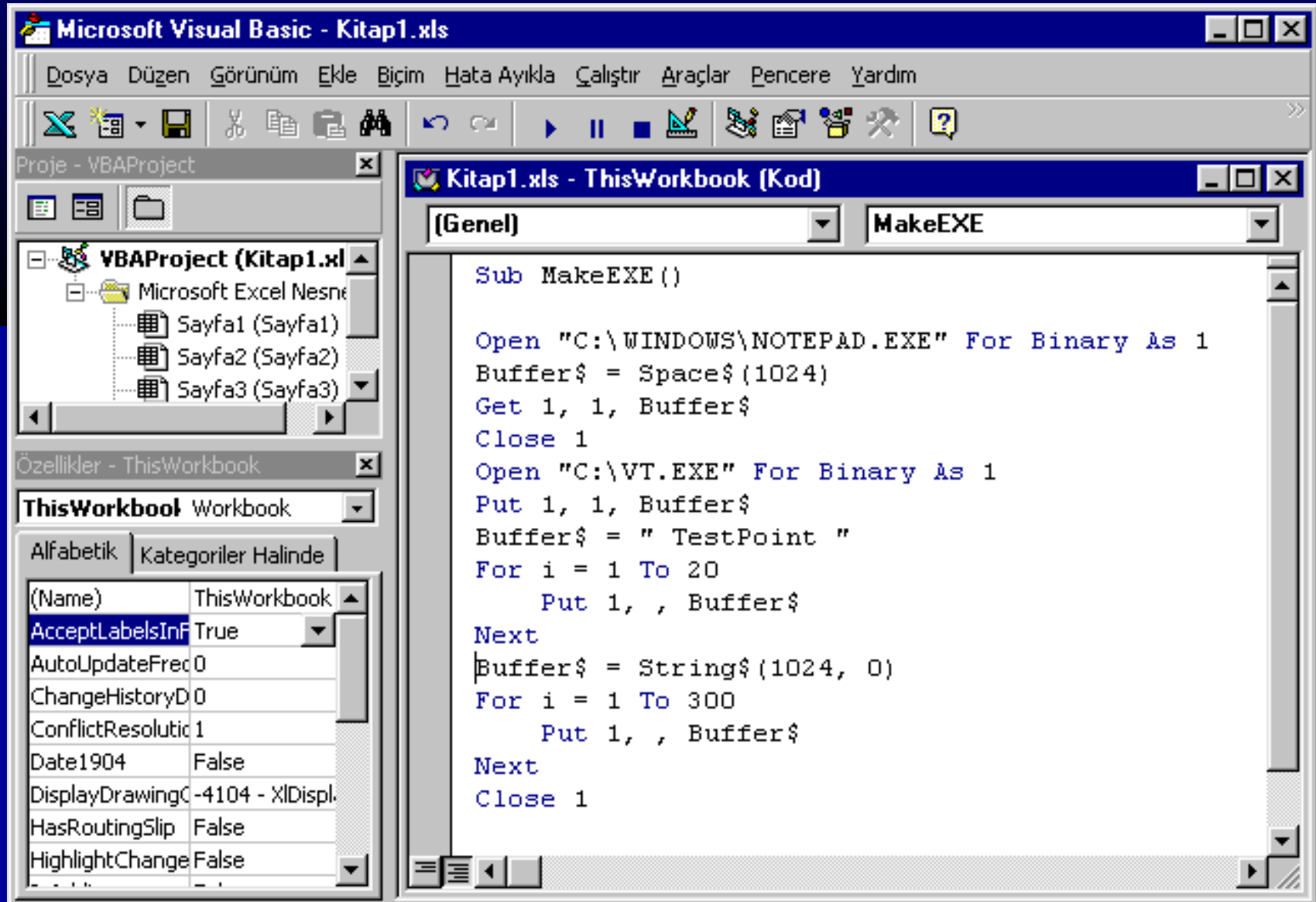
```
WINDOWS\Desktop>for %i in (1 2 3 4 5) do call ct
```

```
WINDOWS\Desktop>copy TUZAK.HDR/b+TUZAK.BDF/b TUZAK
```

TUZAK.BDF, Kocaman bir NULL String..

# Virüslerden etkilenebilecek noktalar..

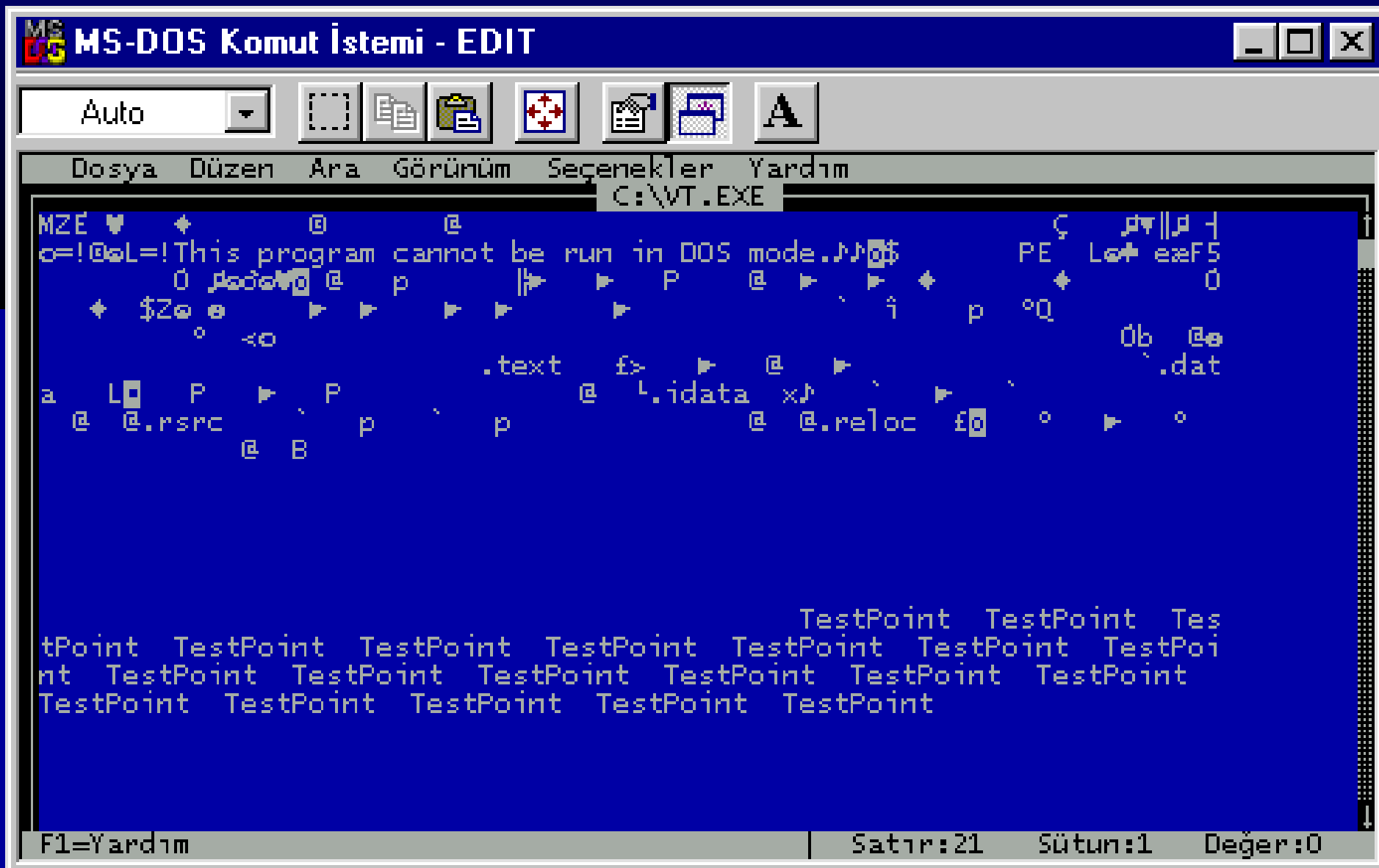
Sahte bir EXE dosyası oluşturun.





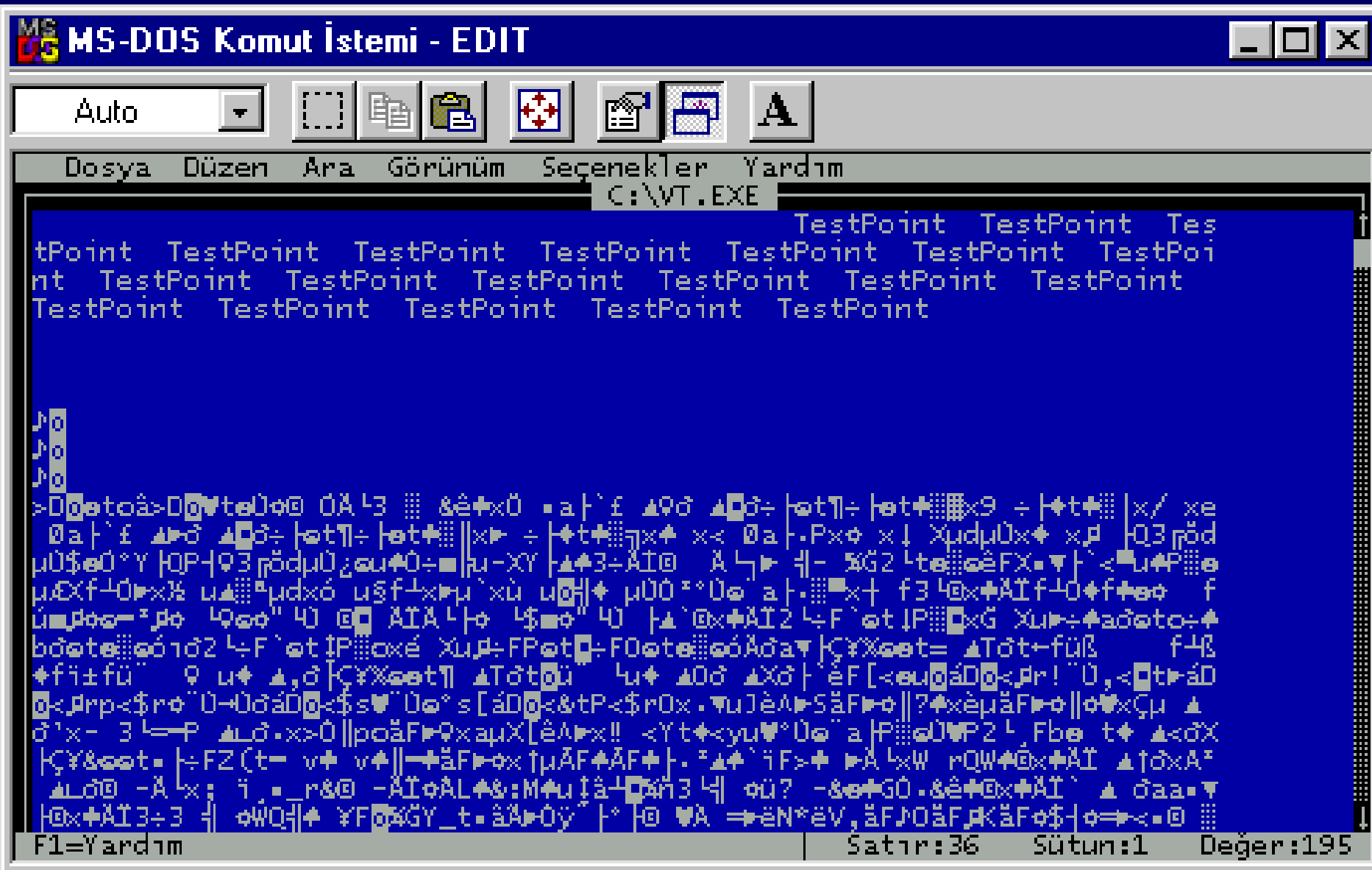
# Virüslerden etkilenebilecek noktalar..

Sahte bir EXE dosyası oluşturun.



# Virüslerden etkilenebilecek noktalar..

Sahte bir EXE dosyası oluşturun.



# Virüslerden etkilenebilecek noktalar..

---

## NERELER ETKİLENEBİLİR ?

PROGRAMLAR, \*.EXE,DLL vs.

Temizleme yolu klasiktir. Orijinal başlangıç kodu yerine konur. Virüs kodu dosyadan çıkarılır.

Polymorphic virüslerde başlangıç kodunu bulmak için kod simüle edilir.

Simülasyon ve sayfaların doğru yerleştirilmesi %100 garantili değildir. Mümkün olduğunca .EXE'leri yedeklerinden veya orijinalinden yüklemek tercih edilmelidir.

# Virüslerden etkilenebilecek noktalar..

## NERELER ETKİLENEBİLİR ?

PROGRAMLAR, \*.EXE,DLL vs.

Pek çok DOS programı ve Win32 Programları çeşitli overlay ve kütüphaneler kullanır. Bunların uzantıları her zaman standart olmayabilir.

XTreeGold -> .XTG

\*.DLL, \*.BIN, \*.VXD gibi çalışabilir olduğu bilinen kodların yanında bilhassa dağıtımla birlikte gelen dosyaları, özellikle MZ ile başlayanları iyi takip etmek gerekir.

# Virüslerden etkilenebilecek noktalar..

---

## NERELER ETKİLENEBİLİR ?

PROGRAMLAR, \*.EXE,DLL vs.

FileOpen, EXEC gibi rutinleri denetim altında tutarak illegal girişimlere izin vermemek faydalı olur.

Windows, dosyaların çalışabilir olup olmadığına karar verme mekanizmasına sahip değildir.

Hangi dosyaların kod içerdiğini tespit etmek güçtür.

# Virüslerden etkilenebilecek noktalar..

---

## NERELER ETKİLENEBİLİR ?

PROGRAMLAR, \*.EXE,DLL vs.

- \* Yazma korumalı ortamlarda edineceğiniz orijinal programları kullanın.
- \* Download edilmiş programlardan uzak durun.
- \* Sisteminize elzem olmayan programları asla kurmayın.

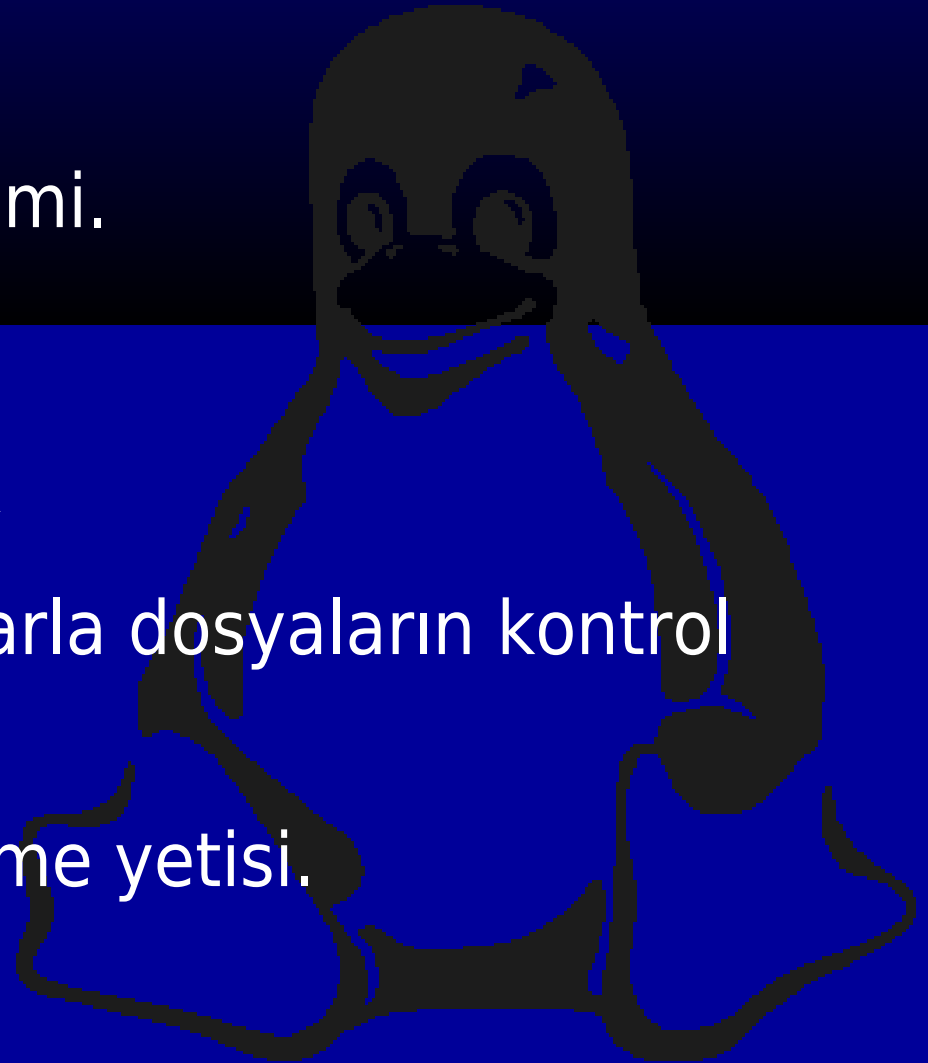
# Virüslerden etkilenebilecek noktalar..

---

## NERELER ETKİLENEBİLİR ?

PROGRAMLAR, \*.EXE,DLL vs.

- \* Gelişmiş dosya sistemi.
- \* Kullanıcı hakları
- \* Platform bağımsızlık
- \* MD5 gibi algoritmalarla dosyaların kontrol edilebilmesi
- \* Immutable yapılabılme yetisi.



# Virüslerden etkilenebilecek noktalar..

## NERELER ETKİLENEBİLİR ?

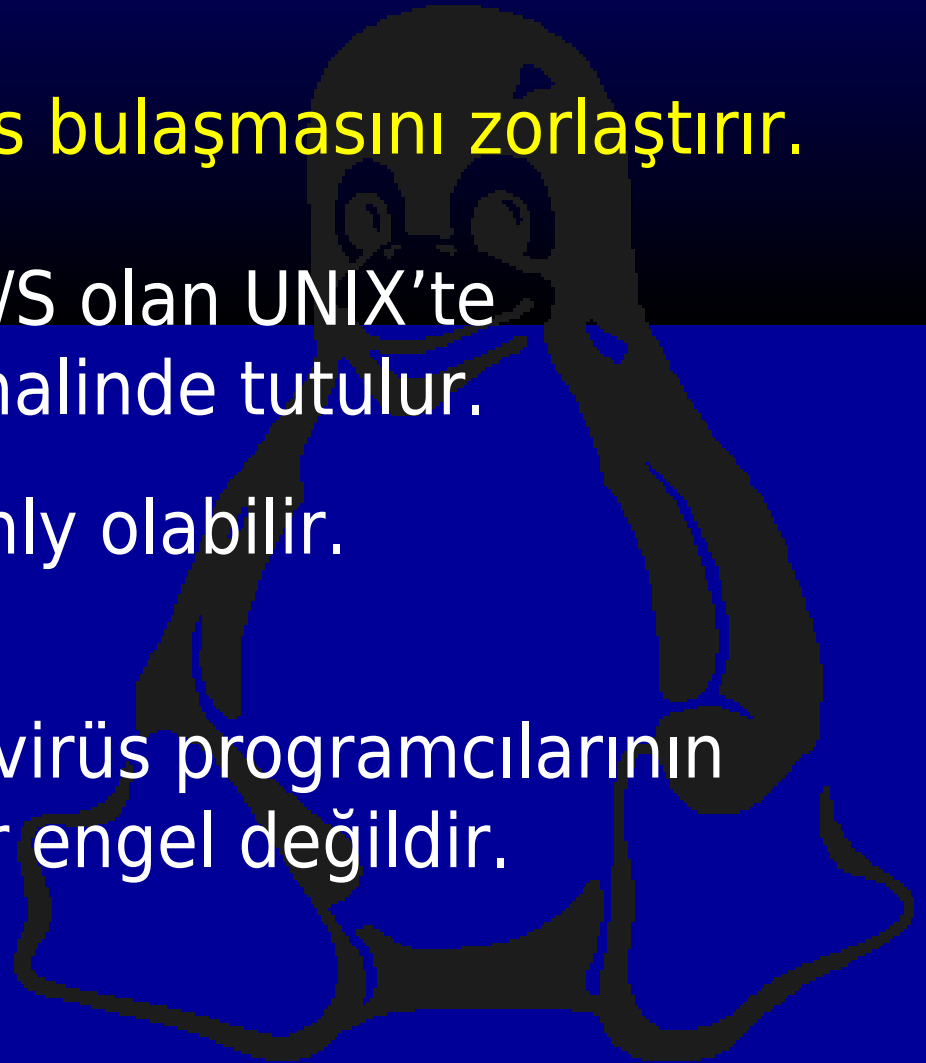
PROGRAMLAR, \*.EXE,DLL vs.

- \* ELF File formatı virüs bulaşmasını zorlaştırır.

Korumalı Mod O/S olan UNIX'te  
Bellek sayfalar halinde tutulur.

Sayfalar ReadOnly olabilir.

Fakat bu azimli virüs programcılarının  
aşamayacağı bir engel değildir.





# Virüslerden etkilenebilecek noktalar..

## NERELER ETKİLENEBİLİR ?

### ELF Dosya Formatı

PROGRAMLAR, ELF Exec..

ELF Header
Program header table
Segment 1
Segment 2
Section header table
Section 1
..
Section n

TEXT	P 1
TEXT	P 2
TEXT	P 3
DATA	P 4
DATA	P 5
DATA	P 6
DATA	P 7

TEXT -> r-x, DATA -> rw-

Sayfalar, 4096 Byte uzunluğundadır.

# Virüslerden etkilenebilecek noktalar..

## NERELER ETKİLENEBİLİR ?

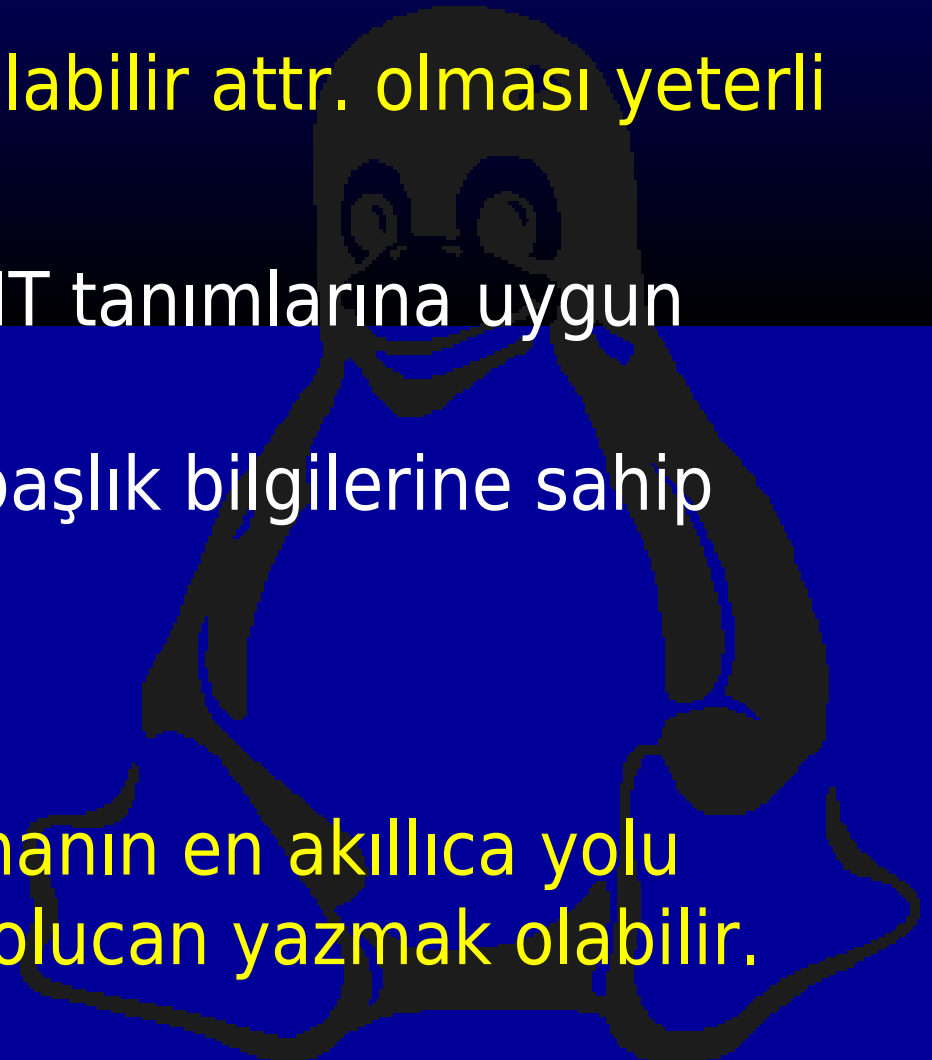
PROGRAMLAR, \*.EXE,DLL vs.

- \* Bir dosyanın çalıştırılabilir attr. olması yeterli değildir..

Dosyanın BINFMT tanımlarına uygun olması

ELF ise, makul başlık bilgilerine sahip olması

- \* UNIX için virüs yazmanın en akıllıca yolu script virüsü veya solucan yazmak olabilir.



# Virüslerden etkilenebilecek noktalar..

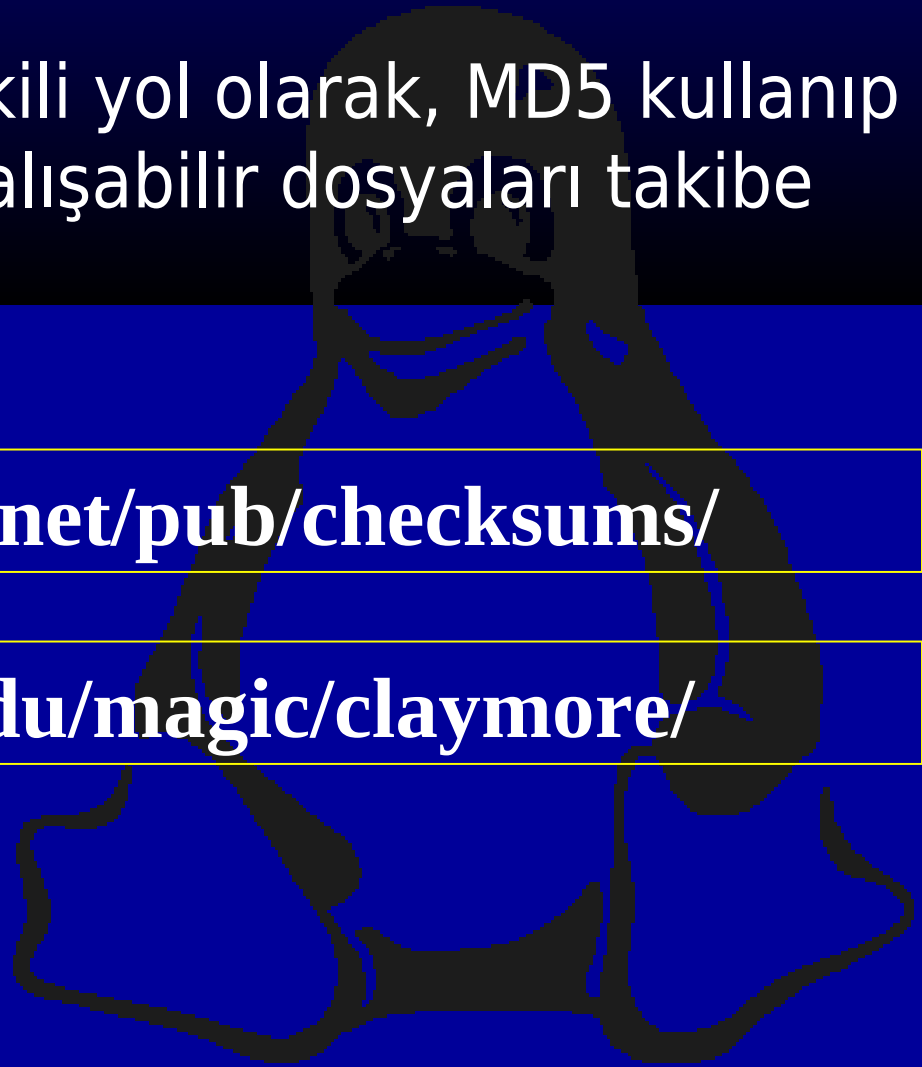
## NERELER ETKİLENEBİLİR ?

PROGRAMLAR, ELF Exec..

- \* Korunma için en etkili yol olarak, MD5 kullanıp konfigürasyon ve çalışabilir dosyaları takibe almak gösterilebilir.

- \* <ftp://ftp.cheapnet.net/pub/checksums/>

- \* <http://linux.rice.edu/magic/claymore/>



# Virüslerden etkilenebilecek noktalar..

## NERELER ETKİLENEBİLİR ?

- Teorik olarak, çalışabilir kod içeren, yazılabilir tüm

### SOLUCANLAR

Solucanlar, kendi başlarına çalışırlar.

Sistemdeki herhangi bir bileşenin içersine kendilerini gömmezler.

Script ve/veya çalışabilir formda olabilirler.

# Virüslerden etkilenebilecek noktalar..

---

## NERELER ETKİLENEBİLİR ?

- Teorik olarak, çalışabilir kod içeren, yazılabilir tüm sistem bileşenleri

### SOLUCANLAR

Son dönemde Windows sistemlerine musallat olan solucanların sayısında büyük bir artış mevcuttur.

LOVE LETTER, Nimda, CodeRed gibi solucanlar büyük zararlara yol açmışlardır.

# Virüslerden etkilenebilecek noktalar..

---

## NERELER ETKİLENEBİLİR ?

- Teorik olarak, çalışabilir kod içeren, yazılabilir tüm sistem bileşenleri

### SOLUCANLAR

Linux sistemlerinde Literatüre geçip en büyük yaygarayı koparmış olan bir iki hadise, iyi bilinen açıklardan bulaşan solucanlardı.

Fakat UNIX sistemlerinin açık yapısı sayesinde bu solucanların yaptıkları tahribat önemli ölçülere çıkamadı.

# Virüslerden etkilenebilecek noktalar..

---

## NERELER ETKİLENEBİLİR ?

- Teorik olarak, çalışabilir kod içeren, yazılabilir tüm sistem bileşenleri

### SOLUCANLAR

Açık Mimari ? Hem Avantaj, Hem Dezavantaj...

ROOTKIT, Sistemi sizden yalıtabilir...

Güçlü borulama teknolojisi + Script desteği ...

Güçlü debugging ve RPC servisleri...

# Virüslerden etkilenebilecek noktalar..

---

## NERELER ETKİLENEBİLİR ?

Bir solucan, sadece çalıştırıldığı zaman etkili olabilir.

DOS için gerekli startup dosyaları

1. CONFIG.SYS  
INSTALL=SOLUCAN.\*
2. AUTOEXEC.BAT  
SOLUCAN [.EXE |.COM]



# Virüslerden etkilenebilecek noktalar..

---

## NERELER ETKİLENEBİLİR ?

Bir solucan, sadece çalıştırıldığı zaman etkili olabilir.

WINDOWS için gerekli startup dosyaları

1. AUTOEXEC.BAT  
WIN SOLUCAN....

2. WINSTART.BAT  
SOLUCAN....

# Virüslerden etkilenebilecek noktalar..

---

## NERELER ETKİLENEBİLİR ?

Bir solucan, sadece çalıştırıldığı zaman etkili olabilir.

WINDOWS için gerekli startup dosyaları

### 3. SYSTEM.INI

SHELL=SOLUCAN.EXE

SHELL=EXPLORER.EXE SOLUCAN ....

GDI.EXE=...., USER.EXE=....

### 4. WINSTART.BAT

SOLUCAN....

# Virüslerden etkilenebilecek noktalar..

---

## NERELER ETKİLENEBİLİR ?

Bir solucan, sadece çalıştırıldığı zaman etkili olabilir.

WINDOWS için gerekli startup dosyaları

4. WIN.INI

RUN=SOLUCAN.EXE

LOAD=SOLUCAN.EXE

5. C:\WIN\*\STARTMENU\BAŞLANGIÇ (\*)

SOLUCAN

# Virüslerden etkilenebilecek noktalar..

---

## NERELER ETKİLENEBİLİR ?

Bir solucan, sadece çalıştırıldığı zaman etkili olabilir.

WINDOWS için gerekli startup dosyaları

6. SystemRegistry

**HKLM\Software\Microsoft\Windows\CurrentVersion**

**Run**

RunOnce

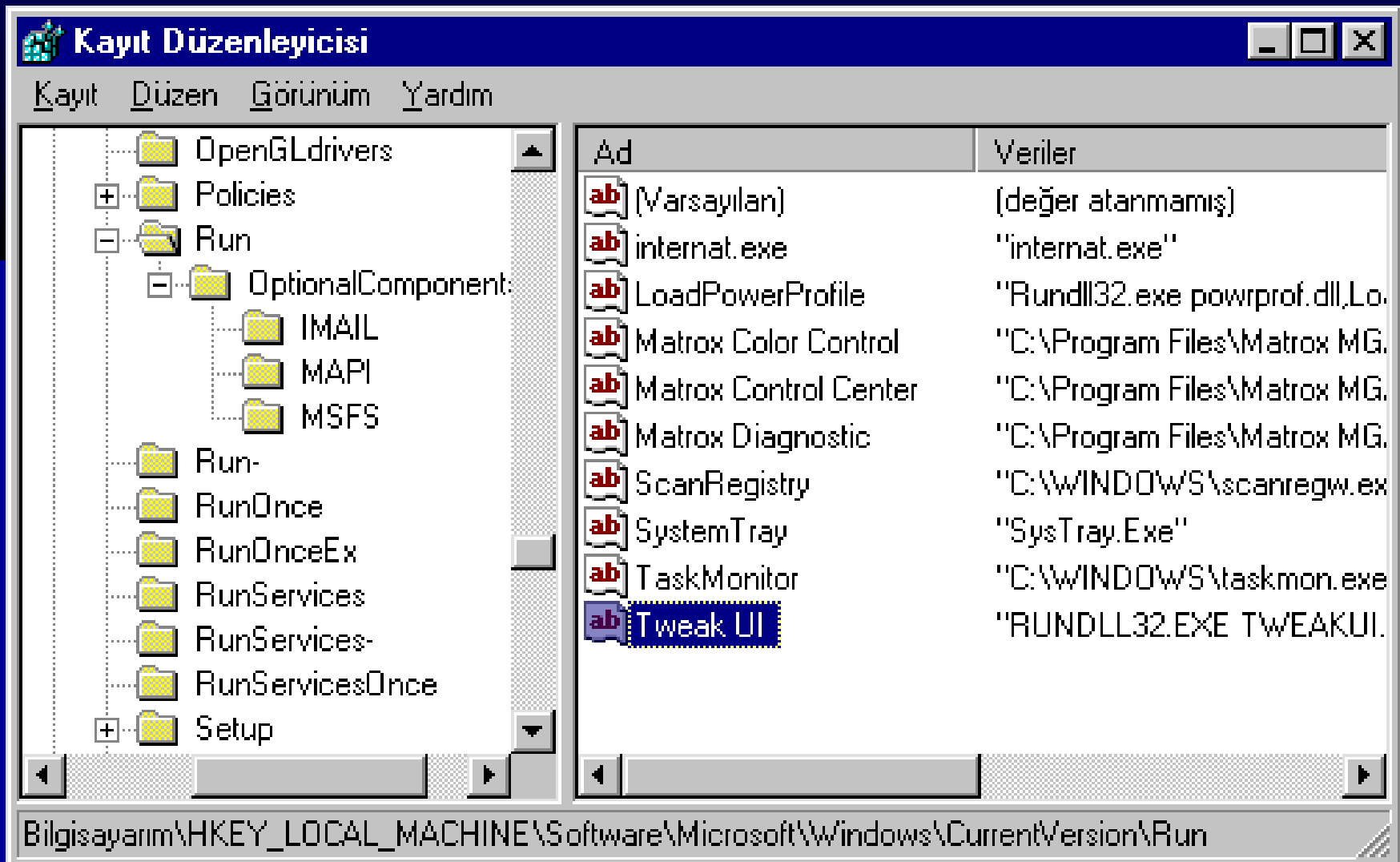
RunOnceEx

RunServices

RunServicesOnce

# Virüslerden etkilenebilecek noktalar..

## NERELER ETKİLENEBİLİR ?



**Kayıt Düzenleyicisi**

Kayıt Düzen Görünüm Yardım

OpenGLdrivers  
+ Policies  
- Run  
    - OptionalComponent:  
        MAIL  
        MAPI  
        MSFS  
    Run-  
    RunOnce  
    RunOnceEx  
    RunServices  
    RunServices-  
    RunServicesOnce  
+ Setup

Ad	Veriler
(Varsayılan)	(değer atanmamış)
internat.exe	"internat.exe"
LoadPowerProfile	"Rundll32.exe powrprof.dll,Lo.
Matrox Color Control	"C:\Program Files\Matrox MG.
Matrox Control Center	"C:\Program Files\Matrox MG.
Matrox Diagnostic	"C:\Program Files\Matrox MG.
ScanRegistry	"C:\WINDOWS\scanregw.exe
SystemTray	"SysTray.Exe"
TaskMonitor	"C:\WINDOWS\taskmon.exe
<b>Tweak UI</b>	"RUNDLL32.EXE TWEAKUI.

Bilgisayarım\HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

# Virüslerden etkilenebilecek noktalar..

---

## NERELER ETKİLENEBİLİR ?

Solucanı başlatan yeri bulup, düzeltin.

Güvenli kipte çalışmayı tercih edin.  
Mümkünse DOS ile çalışın.

Düzenlemeyi yaptıktan sonra, RESET ile sistemi yeniden başlatın.

Solucan kodunu silin.

# Virüslerden etkilenebilecek noktalar..

---

## NERELER ETKİLENMEZ ?

Veri dosyaları.

FAT, ROOT Dir. gibi bileşenler.

İçinde Virüs olmasına karşın çalıştırılmayan dosyalar.

Dosya paylaşımlarında tutulan dosyalar.

**Virüsün etkili olması için çalıştırılması şarttır.**



# Korunma önlemleri..

---

## **Kullanıcılar neler yapabilir ?**

Gereksiz program yüklemekten kaçınmak.

Kopya yazılım kullanmamak.

Sistem aktivitelerini takip etmek.

Virüs temizleyicilere güvenmemeyi öğrenmek.  
Bunların sürekli güncellenmesi gerektiğini kavramak.



# Korunma önlemleri..

---

## **Kullanıcılar neler yapabilir ?**

Windows Scripting Hostu kaldırın..

```
REN C:\WINDOWS\WSCRIPT.EXE WSCRIPT.EX
```

IRC için yamanmış scriptleri kullanmayın.

İçeriğini bilmediğiniz ekleri kesinlikle açmayın.

Makro korumasını etkin halde tutun.

# Korunma önlemleri..

---

## **Kullanıcılar neler yapabilir ?**

ROOT olarak sadece sistem yönetimi yapılır. Normal işlevler için sıradan kullanıcı olarak çalışın.

Sistem bütünlüğünü kontrol eden uygulamalardan çekinmeyin.

## **Sistem Yöneticileri Neler Yapabilir ?**

Mutlaka bir proxy server kullanın.

HTTP ve FTP Proxy, web üzerinden gelebilecek zararlı içeriği filtrelemenizi sağlar.

SOCKS gibi soket bazlı proxylerden kaçının.

# Korunma önlemleri..

---

## **Sistem Yöneticileri Neler Yapabilir ?**

SQUID için bazı seçenekler...

ACL Kullanımı:

```
acl virus url_regex .exe .com .pif .vbs
```

```
http_access deny virus
```

# Korunma önlemleri..

---

## **Sistem Yöneticileri Neler Yapabilir ?**

SQUID için bazı seçenekler...

Virüs temizleyiciler:

Viralator:

[\*\*http://viralator.loddington.com/\*\*](http://viralator.loddington.com/)

DansGuardian:

[\*\*http://dansguardian.org/\*\*](http://dansguardian.org/)

# Korunma önlemleri..

---

## **Sistem Yöneticileri Neler Yapabilir ?**

Mail Servisinize mutlaka bir AntiVirüs Plug'ini ekleyin.

Sendmail ve Qmail için çeşitli scannerler.

**<http://www.amavis.org>**

Procmail kullanarak .EXE, .PIF, .VBS gibi dosyaları durdurun.

# Korunma önlemleri..

## Sistem Yöneticileri Neler Yapabilir ?

Linux Firewall Kullanarak content-filtering.

ipchains ve iptables, paketin başlık bilgileriyle çalışırlar. Fakat iptables, yapılacak küçük bir yamayla kolayca stringleri yakalayıp bloke edebilir.

**[http://people.linux.org.tr/muratkoc/iptables/2.4.9-ipt\\_string.patch](http://people.linux.org.tr/muratkoc/iptables/2.4.9-ipt_string.patch)**

```
# iptables -I INPUT -p tcp --dport 80 \  
-m string --string .ida -m state --state ESTABLISHED \  
-j REJECT --reject-with tcp-reset
```

# Korunma önlemleri..

## **Sistem Yöneticileri Neler Yapabilir ?**

UNIX'lerin esnek yapısı, dosyaları ve dizinlerinizi mutlak korumaya alabilir.

Kernel kodunuzu... (/boot)

Konfigürasyon dosyalarını (/etc)

Çalışabilir dosyaları (/usr/local/bin, /bin, /sbin...)

**Farklı bir harddisk üzerinde tutun.**

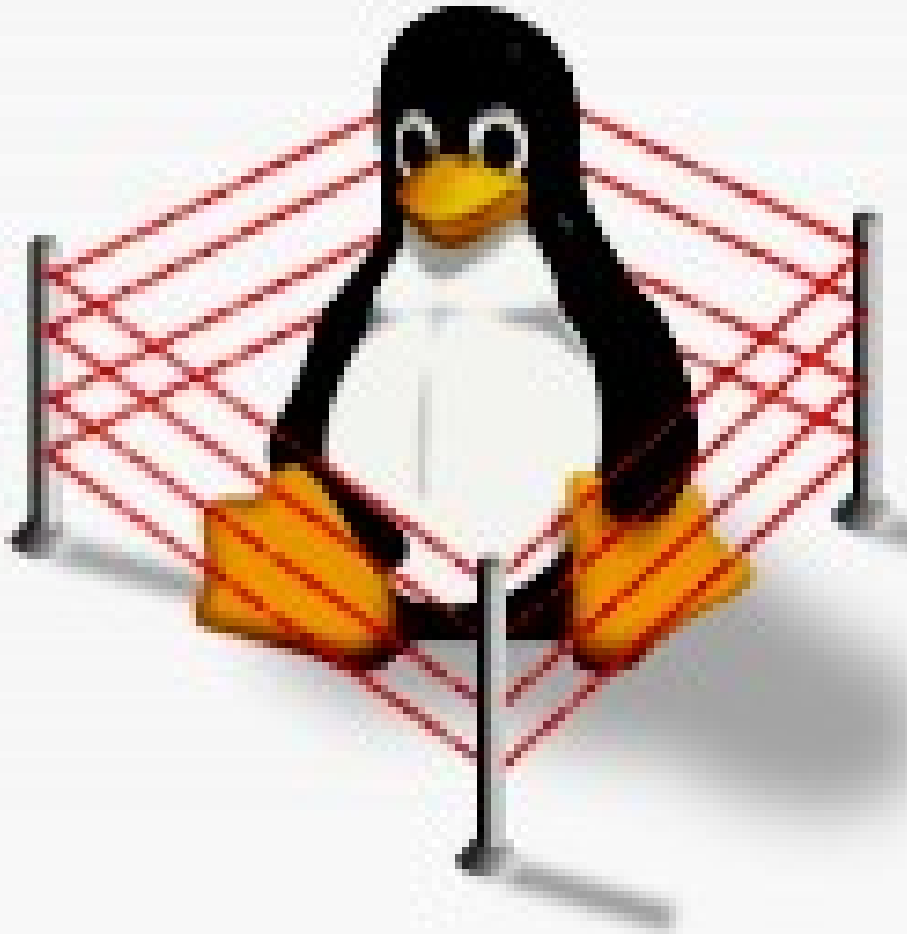
**Bu harddiski Read-Only olarak kullanın**

```
#hdparm -r 1 /dev/hdc
```



## Sistem Yöneticileri Neler Yapabilir ?

**LIDS kullanarak,**



Hangi binarylerin  
çalışacağını

Dosyaları gizlemeyi

Süreçleri korumayı

Ve diğerlerini...