
Front matter

lang: ru-RU

title: Вредоносные программы. Троянские программы

subtitle: Основы информационной безопасности

author:

- Пинегу Б.А.

institute:

- Российский университет дружбы народов, Москва, Россия

i18n babel

babel-lang: russian

babel-otherlangs: english

Formatting pdf

toc: false

toc-title: Содержание

slide_level: 2

aspectratio: 169

section-titles: true

theme: metropolis

header-includes:

- \metroset{progressbar=frametitle,sectionpage=progressbar,numbering=fraction}
- '\makeatletter'
- '\beamer@ignorenonframefalse'
- '\makeatother'

Докладчик

- * Пинегу Белла Александровна

- * Студентка НБИБД-02-22

- * Российский университет дружбы народов

Определение вредоносных программ

Вредоносные программы - специально разработанные для нанесения вреда компьютерной системе, устройству или пользователям. Они могут включать в себя различные типы вредоносных кодов, такие как вирусы, черви, троянские кони, шпионские программы и рекламное ПО.

Зачем создаются троянские программы

- кража личной информации

- удаленное управление компьютером
- вымогательство
- распространение других вредоносных программ
- шпионаж и слежка

Основные виды вредоносных программ

1. Вирусы

2. Черви

```
[bapinega@bapinega ~]$ getenforce
Permissive
[bapinega@bapinega ~]$ sestatus
SELinux status:                enabled
SELinuxfs mount:              /sys/fs/selinux
SELinux root directory:       /etc/selinux
Loaded policy name:            targeted
Current mode:                  permissive
Mode from config file:         enforcing
Policy MLS status:             enabled
Policy deny_unknown status:    allowed
Memory protection checking:    actual (secure)
Max kernel policy version:     33
[bapinega@bapinega ~]$ service httpd start
Redirecting to /bin/systemctl start httpd.service
[bapinega@bapinega ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: enabled)
   Active: active (running) since Wed 2024-02-21 19:47:18 MSK; 8s ago
     Docs: man:httpd.service(8)
   Main PID: 11041 (httpd)
   Status: "Started, listening on: port 80"
```

3. Троянские программы

Троянские программы

это вредоносные программы, которые скрываются под обычными или полезными программами, чтобы получить доступ к компьютеру и выполнить определенные действия без согласия пользователя. В отличие от вирусов, трояны чаще всего направлены на кражу конфиденциальной информации или обеспечение удаленного доступа к компьютеру. Попасть такие программы могут самыми разными способами.

Троянские программы:

1. Backdoor: Этот тип троянского коня открывает "заднюю дверь" в систему, обеспечивая злоумышленнику удаленный доступ к компьютеру.
2. Donald Dick: Троян, который может удалять файлы с компьютера или изменять системные настройки.
3. Crack2000: Троян, используемый для обхода защиты лицензий программного обеспечения.

Троянские программы:

4. Extacis: Троян, который шифрует файлы на компьютере и требует выкуп для их разблокировки.
5. KillCMOS and Netbus: Трояны, используемые для удаленного управления компьютером или вызова различных проблем с системой.

Опасность троянских программ

1. Угроза безопасности данных

```
[bapinega@bapinega ~]$ service httpd start
Redirecting to /bin/systemctl start httpd.service
[bapinega@bapinega ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: enabled)
   Active: active (running) since Wed 2024-02-21 19:47:18 MSK; 8s ago
     Docs: man:httpd.service(8)
   Main PID: 11041 (httpd)
   Status: "Started, listening on: port 80"
    Tasks: 213 (limit: 12167)
   Memory: 23.8M
    CGroup: /system.slice/httpd.service
           └─11041 /usr/sbin/httpd -DFOREGROUND
             11060 /usr/sbin/httpd -DFOREGROUND
             11061 /usr/sbin/httpd -DFOREGROUND
             11063 /usr/sbin/httpd -DFOREGROUND
             11064 /usr/sbin/httpd -DFOREGROUND

фев 21 19:47:13 bapinega.localdomain systemd[1]: Starting The Apache HTTP Server:
фев 21 19:47:18 bapinega.localdomain systemd[1]: Started The Apache HTTP Server:
фев 21 19:47:19 bapinega.localdomain httpd[11041]: Server configured, listening on: port 80
```

2. Подрыв стабильности системы
3. Отслеживание действий пользователя

```
[bapinega@bapinega ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 11041 0.0 0.5 265108 11556 ?
Ss 19:47 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 11060 0.0 0.4 269812 8404 ?
S 19:47 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 11061 0.0 0.7 1458732 14236 ?
Sl 19:47 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 11063 0.0 0.6 1327604 12240 ?
Sl 19:47 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 11064 0.0 0.5 1327604 10200 ?
Sl 19:47 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 bapinega 11479 0.0 0.0 22
1940 1080 pts/1 S+ 19:52 0:00 grep --color=auto httpd
```

Как защититься от троянских программ?

- установка антивируса

```
[bapinega@bapinega ~]$ sestatus -b | grep httpd
httpd_anon_write off
httpd_builtin_scripting on
httpd_can_check_spam off
httpd_can_connect_ftp off
httpd_can_connect_ldap off
httpd_can_connect_mythtv off
httpd_can_connect_zabbix off
httpd_can_network_connect off
httpd_can_network_connect_cobbler off
httpd_can_network_connect_db off
httpd_can_network_memcache off
httpd_can_network_redis off
httpd_can_network_relay off
httpd_can_sendmail off
httpd_dbus_avahi off
httpd_dbus_sssd off
httpd_dontaudit_search_dirs off
httpd_enable_cgi on
```

- обновление ОС и всех установленных программ
- бережное отношение к интернет-ресурсам.
- использовать брандмауэр для контроля сетевого трафика и предотвращения несанкционированного доступа к компьютеру.