

ТОТАЛЬНЕ СПОСТЕРЕЖЕННЯ ЗА ЖУРНАЛІСТАМИ
В РЕДАКЦІЇ “УКРАЇНСЬКОГО ТИЖНЯ”

(кібер-розслідування)



**Головна гіпотеза: журналісти УТ
знаходяться “під ковпаком”.**

**(Параноя, чи обгрунтоване
твердження?)**

Крок перший:
знайти програму-шпигуна

Перша знахідка: програма

servemp.exe

в диспетчері команд Windows

Диспетчер команд

- * викликається клавішами Ctrl-Alt-Del**
- * показує список всіх програм,
що в даний момент
виконуються в системі**

Диспетчер задач Windows

Файл Параметры Вид Завершение работы Справка

Приложения Процессы Быстродействие Сеть Пользователи

Имя образа	Имя пользоват...	ЦП	Память
pod32kpn.exe	SYSTEM	00	18 236 КБ
pod32kui.exe	4_Aнна Babinec	00	1 536 КБ
r_server.exe	SYSTEM	00	2 148 КБ
RTHDCPL.EXE	4_Aнна Babinec	00	11 412 КБ
servemp.exe	4_Aнна Babinec	00	2 828 КБ
services.exe	SYSTEM	00	2 084 КБ
smss.exe	SYSTEM	00	276 КБ
spoolsv.exe	SYSTEM	00	2 312 КБ
svchost.exe	SYSTEM	00	2 720 КБ
svchost.exe	NETWORK SERVICE	00	2 484 КБ
svchost.exe	SYSTEM	00	13 972 КБ
svchost.exe	NETWORK SERVICE	00	2 588 КБ
svchost.exe	LOCAL SERVICE	00	2 316 КБ
svchost.exe	SYSTEM	00	3 960 КБ
System	SYSTEM	00	236 КБ
taskmgr.exe	4_Aнна Babinec	02	4 124 КБ
winlogon.exe	SYSTEM	00	1 184 КБ
Бездействие сис...	SYSTEM	81	28 КБ

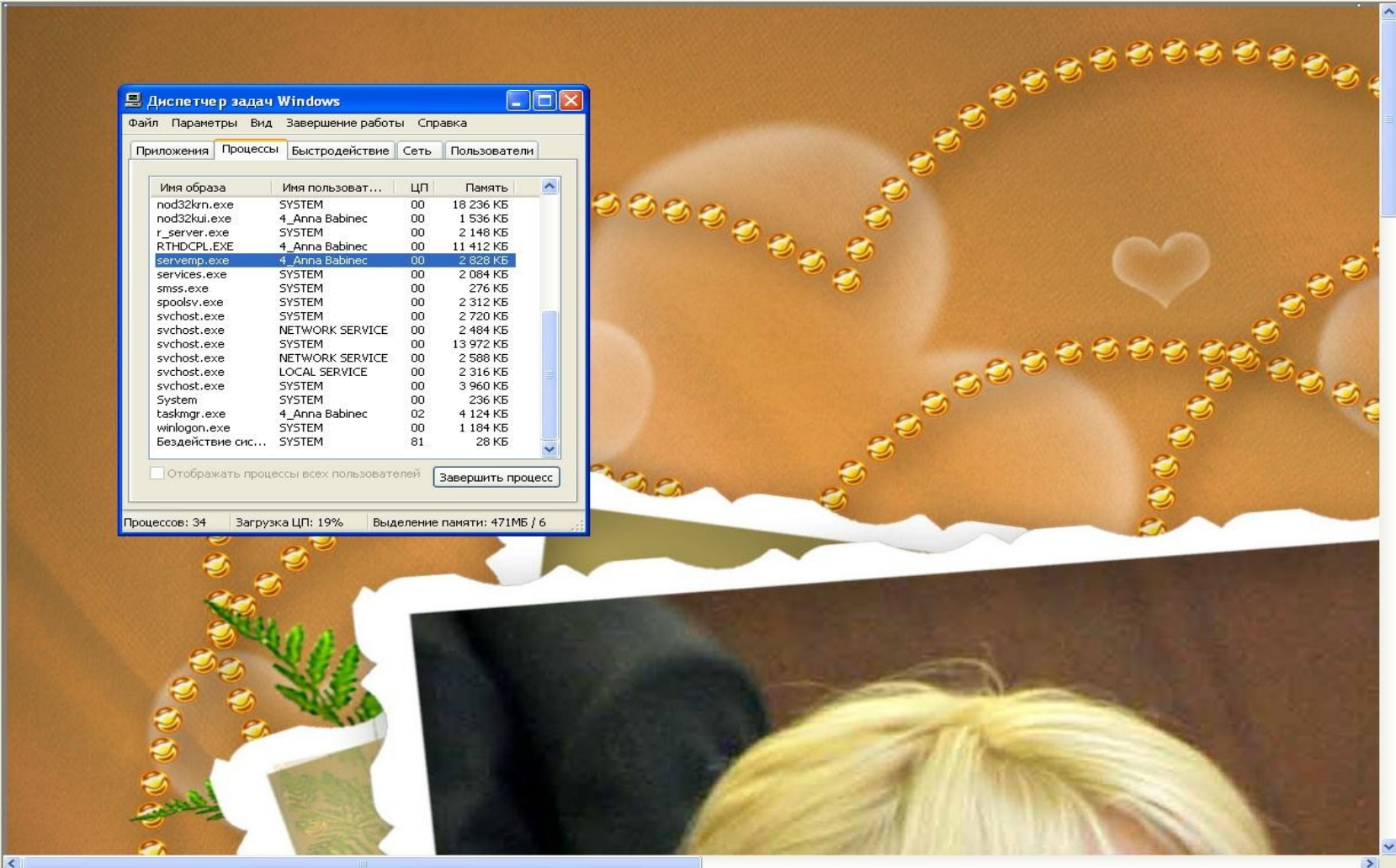
Отображать процессы всех пользователей

Завершить процесс

Процессов: 34

Загрузка ЦП: 19%

Выделение памяти: 471МБ / 6



Диспетчер задач Windows

Файл Параметры Вид Завершение работы Справка

Приложения **Процессы** Быстродействие Сеть Пользователи

Имя образа	Имя пользоват...	ЦП	Память
nod32krn.exe	SYSTEM	00	18 236 КБ
nod32kui.exe	4_Aнна Babinec	00	1 536 КБ
r_server.exe	SYSTEM	00	2 148 КБ
RTHDCPL.EXE	4_Aнна Babinec	00	11 412 КБ
servemp.exe	4_Aнна Babinec	00	2 828 КБ
services.exe	SYSTEM	00	2 084 КБ
smss.exe	SYSTEM	00	276 КБ
spoolsv.exe	SYSTEM	00	2 312 КБ
svchost.exe	SYSTEM	00	2 720 КБ
svchost.exe	NETWORK SERVICE	00	2 484 КБ
svchost.exe	SYSTEM	00	13 972 КБ
svchost.exe	NETWORK SERVICE	00	2 588 КБ
svchost.exe	LOCAL SERVICE	00	2 316 КБ
svchost.exe	SYSTEM	00	3 960 КБ
System	SYSTEM	00	236 КБ
taskmgr.exe	4_Aнна Babinec	02	4 124 КБ
winlogon.exe	SYSTEM	00	1 184 КБ
Бездействие сис...	SYSTEM	81	28 КБ

Отображать процессы всех пользователей

Процессов: 34 Загрузка ЦП: 19% Выделение памяти: 471МБ / 6



Для получения справки выберите команду "Вызов справки" из меню "Справка".

257,415



servemp.exe

[Складний пошук](#)
[Налаштування](#)
[Мовні інструменти](#)

Пошук Google

Мені пощастить

Пошук: Інтернет сторінки українською мовою сторінки з України

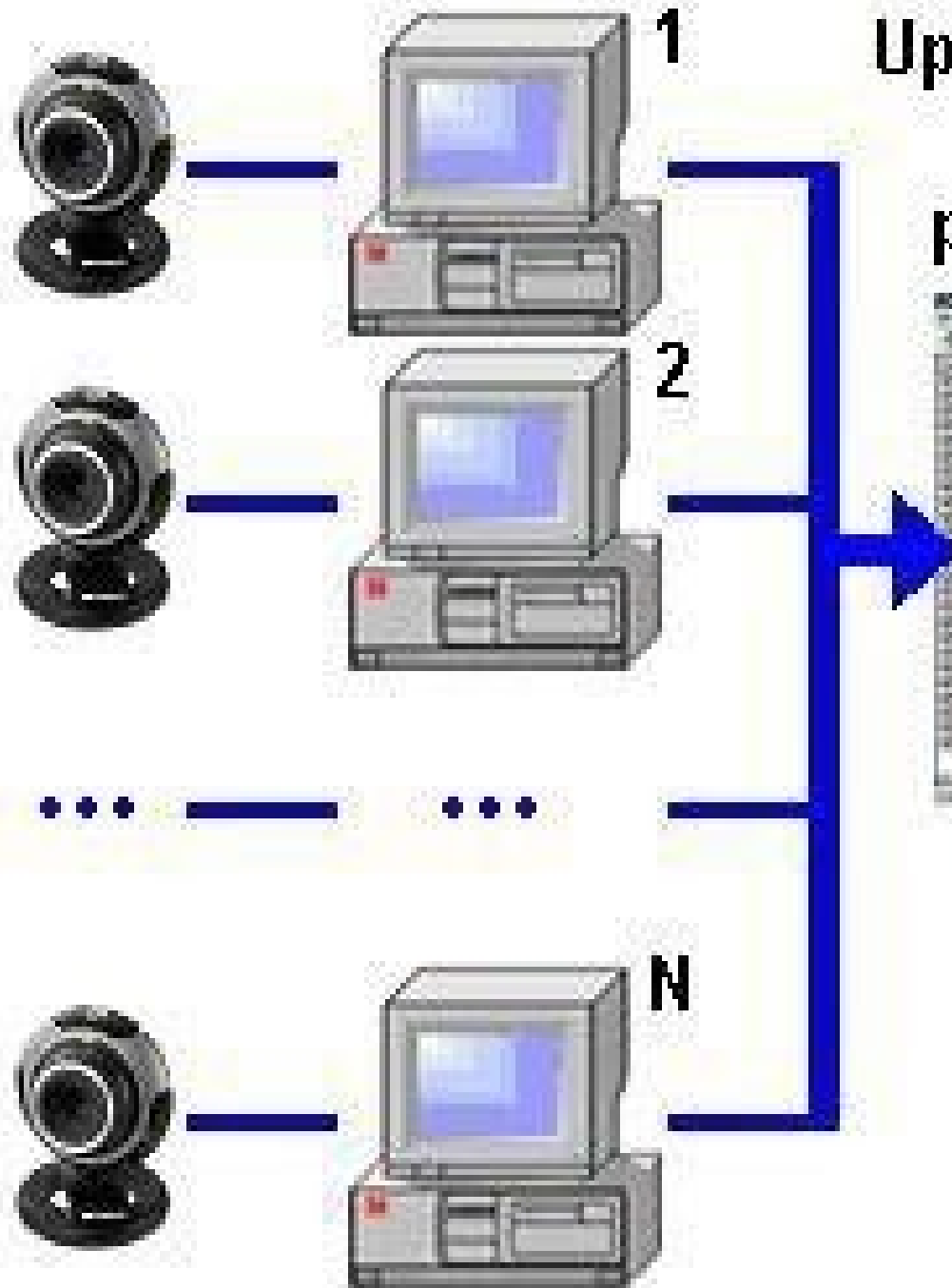
Google.com.ua на [русском](#)

[Рекламні програми](#) - [Все про Google](#) - [Google.com in English](#)

©2009 Google



Up to 250 PCs & WebCams
simultaneously
per 1 manager's PC



Soft.Iron-Ball.Ru

Добра штука ...

- ✔ Поддерживает до 250-ти компьютеров служащих одновременно с одного компьютера менеджера
- ✔ Наблюдение в режиме реального времени и off-line режиме
- ✔ Работает в режимах Запись и Просмотр + слайдшоу скриншотов
- ✔ Прослушивание через микрофоны
- ✔ Интервал захвата экрана: от 2-х секунд до 1-го часа
- ✔ Удалённое управление, 2 режима
- ✔ Поддержка USB вебкамер
- ✔ Офф-лайн счетчик рабочего времени
- ✔ Многоэкранный режим позволяет видеть до 250-ти экранов служащих одновременно на одном экране менеджера (от 2x2 до 16x16)
- ✔ Для сортировки и упорядочивания служащих в программе предусмотрено 25 групп
- ✔ Внешний просмотрщик архива с фильтром по времени удобен для просмотра больших архивов
- ✔ Сохранение скриншотов в любой архивной папке в локальной сети
- ✔ Экономный захват экрана: программа не делает снимки экрана при включенном скринсейвере или при активном режиме пониженного энергопотребления ("сон"), также, не передаются одинаковые скриншоты
- ✔ Возможность подключения через Pгоху
- ✔ Поддержка подключения к компьютерам служащих через Интернет через службы [Dynamic DNS](http://www.dyndns.com), типа www.dyndns.com , www.thatip.com и прочие
- ✔ Режимы автоматического запуска записи
- ✔ Защита паролем
- ✔ Шифрование
- ✔ Передача текстовых сообщений одному служащему, группе служащих, всем сразу
- ✔ Скрытый режим
- ✔ Быстрая установка из командной строки с ключами

Последние изменения (Версия 2.29, Сентября 2008 г.)

- ✔ Наблюдение в режиме реального времени с записью и без записи

Основні можливості:

- * Підглядання за екраном комп'ютера в режимі реального часу або із записом на диск**
- * Підглядання за працівниками за допомогою веб-камери**
- * Підслуховування за допомогою вмонтованого в комп мікрофону**
- * Керування комп'ютером працівника на відстані**

І не дорого!

Softkey-Россия: Ваша корзина - Mozilla Firefox


File Edit View History Bookmarks Wired-Marker Tools Help

http://www.softkey.ru/catalog/basket.php

del.icio.us Open list - Wikipedia, IJZS 2.3 - Zizek on Vi... 4.3. Класифікація ви... JavaScript Visual Wor... Readability QRCode!

Addresses Contacts Events Locations Tagspaces Bookmarks Resources Options


Слежение за ком... servemp.exe - D... Олеансофт: Куп... Олеансофт: Скр... Олеансофт: Ска... Softkey-Россия: ...




SOFTKEY Интернет-магазин программного обеспечения


Найти программу: Пример: [Антивирус Касперского](#) [Расширенный поиск](#)

Ваша корзина


В вашей корзине **1** товар 

Содержимое корзины


Продукт	Поставка	Кол-во	Скидка	Сумма	Отложить	Удалить
Скрытая Камера	E-Mail	<input type="text" value="100"/>		12 869.00 грн. 	<input type="checkbox"/>	<input type="checkbox"/>

Валюта заказа: Рубли Гривны Белорусские рубли Тенге 

Итого: **12 869.00 грн.**


 Если вы изменили количество, отметили флажки "Отложить", "Удалить", "Записать на компакт-диск" или изменили валюту заказа — нажмите на кнопку [Пересчитать](#).

Шаг 1. Информация для оформления заказа


 Вы можете перейти в [защищенный режим](#), который обеспечивает надежное шифрование передаваемых на сервер данных.

Авторизация и тип плательщика



Если вы зарегистрированы на сервере Софткей. При регистрации вы можете указать свое имя входа и пароль. Если вы ничего не указали, то имя входа и


Авторизация 

Имя входа и пароль будут сгенерированы автоматически.

Впервые на Softkey?  [Как заказать](#)

Всего заказов: 1 918 811

 [LiveID](#)  [OpenID](#)

 [Google ID](#)

логин:

пароль:


запомнить

[Регистрация](#)
[Забыли пароль?](#)

Раздел покупателя

[Войти](#)

[Магазин](#)

Done  1 Error

**Отже,
servemp.exe це
програма-шпигун**

Припущення:
програма-шпигун стоїть лише
на одному комп'ютері в офісі
(Підказка: ні, це не так!)

Три інструмента командної строки:

- netstat**
- nmap**
- nbtscan**

(без них дослідження було б неможливим)

IP-адреса

(4 числа через точку)

приклади

195.17.88.12

10.10.10.1

192.168.0.56

217.20.163.85 - УНІАН!

Порт (port) (одне число)

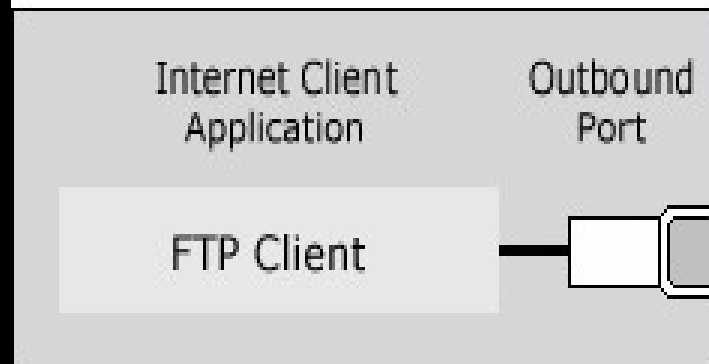
приклади:

80 – вебсервер

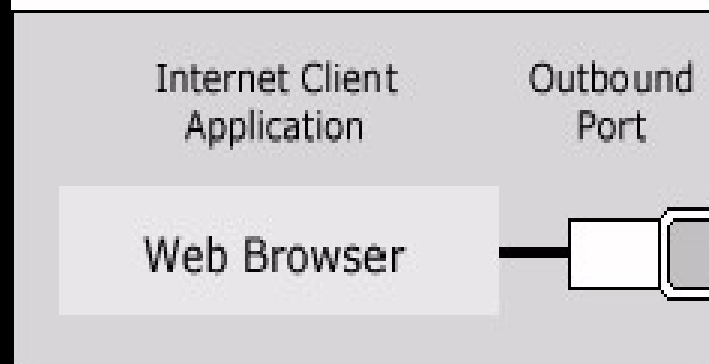
25 – поштовий сервер

21 - FTP

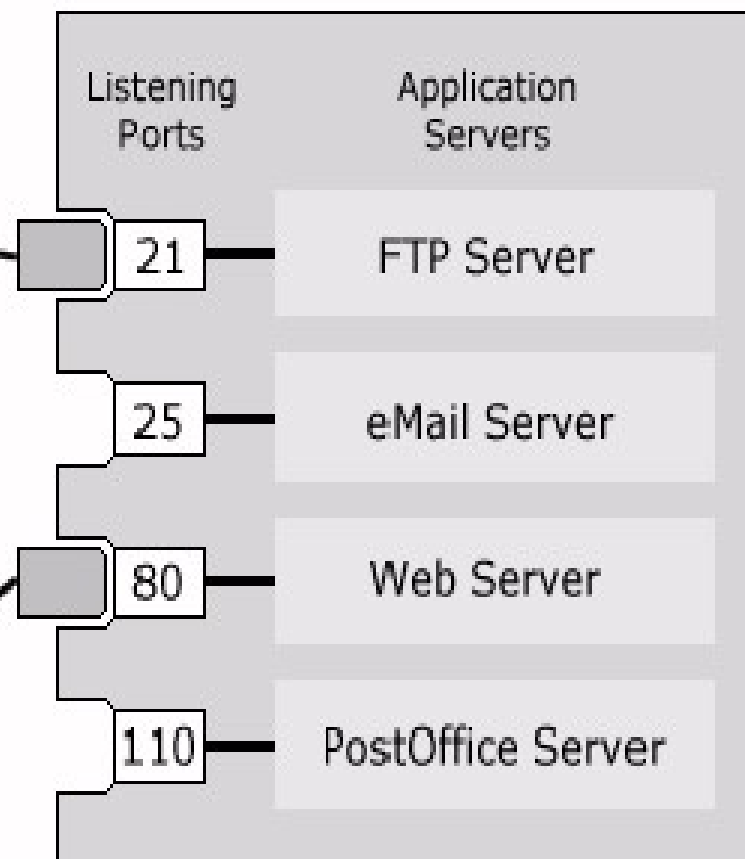
Jack's PC on the Internet



Jill's PC on the Internet



Big Internet Machine



**IP-адреса дозволяє знайти в мережі
окремий комп'ютер**

**Однак на компі може виконуватися
одночасно декілька програм**

**Вони з'єднуються з іншими програмами
на інших компах**

Як вони знаходять один одного?

**За допомогою двох параметрів -
IP-адреси та порта**

наприклад

192.168.1.1:3278 – повна адреса вашого веб-браузера

IP-адреса та порт

однозначно

**визначають координати
будь якої програми
на комп'ютері, що має
вихід в інет**

netstat – стандартна команда Windows

За її допомогою можна отримати інформацію про всі мережеві з'єднання, які робить ваш комп'ютер

... іншими словами

netstat дає відповідь на питання - яка програма з вашого компа ходить в інет, і куди саме? Тобто на який комп'ютер?

**КРОК другий:
з якого компа керують
програмою-шпигуном?**

Результати роботи netstat

```
Microsoft Windows XP [Версия 5.1.2600]
(C) Корпорация Майкрософт, 1985-2001.

C:\Documents and Settings\4_Aнна Babinec>netstat -anb -p TCP

Активные подключения

Имя      Локальный адрес      Внешний адрес      Состояние      PID
TCP      0.0.0.0:135           0.0.0.0:0          LISTENING      980
Не удается получить сведения о владельце
TCP      0.0.0.0:445           0.0.0.0:0          LISTENING      4
Не удается получить сведения о владельце
TCP      0.0.0.0:1045          0.0.0.0:0          LISTENING      2584
Не удается получить сведения о владельце
TCP      0.0.0.0:4010          0.0.0.0:0          LISTENING      1932
[server.exe]

TCP      0.0.0.0:4011          0.0.0.0:0          LISTENING      1932
[server.exe]

TCP      0.0.0.0:4899          0.0.0.0:0          LISTENING      372
Не удается получить сведения о владельце
TCP      127.0.0.1:1031        0.0.0.0:0          LISTENING      512
Не удается получить сведения о владельце
TCP      192.168.0.30:139      0.0.0.0:0          LISTENING      4
Не удается получить сведения о владельце
TCP      127.0.0.1:1059        127.0.0.1:1060     ESTABLISHED     3372
[firefox.exe]

TCP      127.0.0.1:1060        127.0.0.1:1059     ESTABLISHED     3372
[firefox.exe]

TCP      127.0.0.1:1062        127.0.0.1:1063     ESTABLISHED     3372
[firefox.exe]

TCP      127.0.0.1:1063        127.0.0.1:1062     ESTABLISHED     3372
[firefox.exe]

TCP      192.168.0.30:1046     64.12.24.188:5190  ESTABLISHED     2440
[ICQ.exe]

TCP      192.168.0.30:1291     74.125.87.83:443   ESTABLISHED     3372
[firefox.exe]

TCP      192.168.0.30:1292     74.125.87.83:443   ESTABLISHED     3372
[firefox.exe]

TCP      192.168.0.30:4010     192.168.0.232:3698 ESTABLISHED     1932
[server.exe]

TCP      192.168.0.30:1260     74.125.87.83:443   TIME_WAIT       0

C:\Documents and Settings\4_Aнна Babinec>
```



- iTunesSetup
- cherniy_dac...
- msicuu2
- #15_polit_...
- ky_30.03
- #15_tendence



Командная строка

Microsoft Windows XP [Версия 5.1.2600]
 (C) Корпорация Майкрософт, 1985-2001.

C:\Documents and Settings\4_Anna Babinec>netstat -anb -p TCP

Активные подключения

Имя	Локальный адрес	Внешний адрес	Состояние	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	980
Не удается получить сведения о владельце				
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
Не удается получить сведения о владельце				
TCP	0.0.0.0:1045	0.0.0.0:0	LISTENING	2584
Не удается получить сведения о владельце				
TCP	0.0.0.0:4010	0.0.0.0:0	LISTENING	1932
[servemp.exe]				
TCP	0.0.0.0:4011	0.0.0.0:0	LISTENING	1932
[servemp.exe]				
TCP	0.0.0.0:4899	0.0.0.0:0	LISTENING	372
Не удается получить сведения о владельце				
TCP	127.0.0.1:1031	0.0.0.0:0	LISTENING	512
Не удается получить сведения о владельце				
TCP	192.168.0.30:139	0.0.0.0:0	LISTENING	4
Не удается получить сведения о владельце				
TCP	127.0.0.1:1059	127.0.0.1:1060	ESTABLISHED	3372
[firefox.exe]				
TCP	127.0.0.1:1060	127.0.0.1:1059	ESTABLISHED	3372
[firefox.exe]				
TCP	127.0.0.1:1062	127.0.0.1:1063	ESTABLISHED	3372
[firefox.exe]				
TCP	127.0.0.1:1063	127.0.0.1:1062	ESTABLISHED	3372
[firefox.exe]				
TCP	192.168.0.30:1046	64.12.24.188:5190	ESTABLISHED	2440
[ICQ.exe]				
TCP	192.168.0.30:1291	74.125.87.83:443	ESTABLISHED	3372
[firefox.exe]				
TCP	192.168.0.30:1292	74.125.87.83:443	ESTABLISHED	3372
[firefox.exe]				
TCP	192.168.0.30:4010	192.168.0.232:3698	ESTABLISHED	1932
[servemp.exe]				
TCP	192.168.0.30:1260	74.125.87.83:443	TIME_WAIT	0

C:\Documents and Settings\4_Anna Babinec>

TCP	192.168.0.30:1292	74.125.87.83:443	ESTABLISHED	3372
	[firefox.exe]			
TCP	192.168.0.30:4010	192.168.0.232:3698	ESTABLISHED	1932
	[servemp.exe]			

результат роботи netstat

порт № 4010

**саме його використовує програма-шпигун
на нашому комп'ютері**

результат роботи netstat

192.168.0.232 -

адреса комп'ютера,

для якого працює наша програма-шпигун

результат роботи netstat

192.168.0.232 -

**– це один з основних файлових
серверів, що використовуються в офісі УТ**

**шпигунська інформація збирається
на сервері
Українського Тижня**

КРОК 3

де ми даємо відповідь

**За ким ще слідкують
в офісі УТ?**

КРОК 3

де ми даємо відповідь

**За ким ще слідкують
в офісі УТ?**

*** Можна шукати через диспетчер задач вручну, на кожному компі**

*** але краще шукати комп'ютери, у яких так само як на нашому, порт №4010 – є відкритим.**

Це означатиме, що на них також працюють програми-шпигуни!

Але чому саме порт № 4010 ???

**по-перше, саме на ньому
ви вже знайшли програму шпигуна
servemp.exe**

а по друге ...

"Скрытая камера" Hidden camera 250X1 удаленное наблюдение и управление компьютером :: torrents.ru - Mozilla Firefox

File Edit View History Bookmarks Wired-Marker Tools Help

http://torrents.ru/forum/viewtopic.php?t=1350017

del.icio.us Open list - Wikipedia,... IJZS 2.3 - Zizek on Vi... 4.3. Класифікація ви... JavaScript Visual Wor... Readability QRCode!

Addresses Contacts Events Locations Tagspaces Bookmarks Resources

Олеансофт Скр... servemp.exe - D... Google "Скрытая камер..." "Скрытая камер..." Олеансофт Скр...

6. Быстрая установка из командной строки:

- Скопируйте на локальный диск или в папку файл <servemp_quicksetup.exe> из папки <Быстрый установщик модуля служащего> в дистрибутиве программы.
- Запустите его из командной строки с параметрами: `servemp_quicksetup.exe ps=XXX port=N hide=1`
- XXX - пароль для модуля служащего, длина пароля должна быть менее 32 знаков без пробелов. Этот же пароль используйте на компьютере менеджера в настройках камеры для данного служащего. Без ключа "ps=" пароль будет пустым.
- N - порт для соединения через сеть от 3 до 65535, если пропустить ключ "port=", порт будет 4010 по умолчанию.
- Если Вы хотите установить модуль служащего в невидимом режиме, укажите ключ "hide=1"

7. Примечание: на компьютере служащего программа Скрытая Камера будет автоматически загружаться при каждом включении компьютера.

Язык интерфейса: только английский

Таблетка: Присутствует

Find: Next Previous Highlight all Match case

Done

**Лінивi адміни –
це корисно!**

**Як знайти всі комп'ютери
в мережі, у яких порт 4010 -
відкритий?**

ntar

найкращий у світі сканер портів
(є варіанти під Windows, Linux , Mac)

результати роботи nmap:

```
sting: ~ - Terminator
+ost: 192.168.0.43 () Ports: 4010/closed/tcp/////
+ost: 192.168.0.44 () Ports: 4010/filtered/tcp/////
+ost: 192.168.0.56 () Ports: 4010/open/tcp/////
+ost: 192.168.0.67 () Ports: 4010/closed/tcp/////
+ost: 192.168.0.71 () Ports: 4010/open/tcp/////
+ost: 192.168.0.73 () Ports: 4010/open/tcp/////
+ost: 192.168.0.77 () Ports: 4010/closed/tcp/////
+ost: 192.168.0.78 () Ports: 4010/open/tcp/////
+ost: 192.168.0.82 () Ports: 4010/open/tcp/////
+ost: 192.168.0.84 () Ports: 4010/filtered/tcp/////
+ost: 192.168.0.89 () Ports: 4010/open/tcp/////
+ost: 192.168.0.111 () Ports: 4010/open/tcp/////
+ost: 192.168.0.112 () Ports: 4010/closed/tcp/////
+ost: 192.168.0.114 () Ports: 4010/closed/tcp/////
+ost: 192.168.0.116 () Ports: 4010/open/tcp/////
+ost: 192.168.0.146 () Ports: 4010/open/tcp/////
+ost: 192.168.0.177 () Ports: 4010/closed/tcp/////
+ost: 192.168.0.189 () Ports: 4010/closed/tcp/////
+ost: 192.168.0.232 () Ports: 4010/closed/tcp/////
+ost: 192.168.0.250 () Ports: 4010/closed/tcp/////
+ost: 192.168.0.253 () Ports: 4010/closed/tcp/////
# Nmap done at Fri Apr 24 16:11:24 2009 -- 256 IP addresses (40 hosts up) scanned in 1.773 seconds
```

**результати
роботи nтар:**

**з 40 працюючих на момент
перевірки комп"ютерів,
на 24 присутні програми-шпигуни.**

**Серед тих, за ким ведеться
тотальне спостереження
не лише журналісти, але й
рекламісти, і служба розповсюдження**

**КРОК 4 -
назвіть їх поіменно – хто об’єкти
спостереження?**

**Для цього ми використали третій
з названих інструментів для аудиту мереж:
програму**

nbtscan

nbtscan

**показує за IP-адресами
імена комп'ютерів в локальній
мережі Windows**



Серед об'єктів спостереження:

- більшість комп'ютерів журналістів "Тижня"**
- комп'ютери декількох редакторів відділів**
- комп'ютер головного редактора!
(сюрприз)**

Дякую всім, хто допомагав

збирати докази:

- скріншоти**
- логи програм**
- контрольні суми файлів**
- тощо**

**Як подивитися, чи немає
у вас на комп'ютері “черв'яків”, вірусів або
“шпигунів”?**

**Наберіть в командній строці Windows
команду**

netstat -anb -p TCP

**вона покаже програми,
що виходять в мережу з
вашого комп'ютера. Слідкуйте за появою
паразитів типу “servemp.exe”**

Дякую за увагу!

питання:

devrand@gmail.com

