Описание работы вируса Backdoor.Win32. Buterat.afj

antivirnews.blogspot.com/2011/01/backdoorwin32-buteratafj.html

Вредоносная программа, предоставляющая злоумышленнику удаленный доступ к зараженной машине. Является приложением Windows (PE-EXE файл). Имеет размер 89088 байт. Упакована неизвестным упаковщиком. Распакованный размер – около 181 КБ. Написана на C++.

Инсталляция

После запуска бэкдор копирует свое тело в файл:

```
%APPDATA%\netprotocol.exe
```

При этом для противодействия сигнатурным анализаторам антивирусных программ, в копии модифицируются 2 байта:
Подвергнутая подобной модификации копия детектируется Антивирусом Касперского как "Trojan-PSW.Win32.Qbot.aem". Для автоматического запуска созданной копии при каждом следующем старте системы создается ключ системного реестра:

```
[HKLM\Software\Microsoft\Windows\CurrentVersion\Run]
"Netprotocol" = "%APPDATA%\netprotocol.exe"
```

Если данный ключ создать не удается, бэкдор создает ключ:

```
[HKCU\Software\Microsoft\Windows\CurrentVersion\Run]
"Netprotocol" = "%APPDATA%\netprotocol.exe"
```

После этого бэкдор запускает созданную копию на выполнение.

Деструктивная активность

Бэкдор способен копировать свое тело в файл:

```
%WorkDir%\netprotocol.dll
```

и, используя экспортируемую функцию "_ClearEvent@12", внедрять в адресное пространство процессов браузеров:

```
firefox.exe
iexplore.exe
opera.exe
```

исполняемый код, перехватывающий вызовы API-функций:

```
WSARecv
recv
send
```

библиотеки "ws2_32.dll". Таким образом, бэкдор получает возможность следить за входящим и исходящим трафиком браузеров, и по команде злоумышленника собирать информацию о поисковых запросах пользователя на сайты:

```
http://rupoisk.ru
http://ru.search.yahoo.com
http://www.bing.com
http://nigma.ru
http://search.qip.ru
http://nova.rambler.ru
http://www.google.ru
http://yandex.ru
```

а также перенаправлять пользователя на следующие ресурсы:

```
http://aut***gun.ru
http://sear***tnik1.ru
http://autoc***gun.ru
http://ppc***gun.ru
```

Также по команде злоумышленника бэкдор может обновлять свой исполняемый файл, загружая обновление с сервера злоумышленника. Кроме того, может загружаться файл, сохраняемый в рабочем каталоге бэкдора как:

```
%WorkDir%\netprotdrvss
```

После успешной загрузки файл запускается на выполнение. Запросы к серверу злоумышленника, к примеру, могут иметь следующий вид:

- успешная установка бэкдора в системе:

  ```
  /nconfirm.php?rev=294&code=3 m=2&num=
  40401870851072
  ```

- запрос на получение команды:

  ```
  /njob.php?num=&rev=294
  ```

- запрос на загрузку файла "netprotdrvss":

  ```
  /nconfirm.php?rev=294&code=7 m=0&num
  =40401870851072
  ```

Число "" генерируется на основе текущего системного времени. Подстрока "" – имя сервера злоумышленника, может принимать значения:

```
http://sjd***sla.com
http://sa***d.com
http://se***nd.com
http://ha***rd.net
http://he***cy.com
```

На момент создания описания подключиться к указанным серверам не удалось. Имена команд, обрабатываемых бэкдором:

```
ZORKASITE
ZORKAFEED
BODYCLICK
KEYWORDS
RUPFEED
RUPPUBL
XMLFEED
REKLOSOFT
TEASERNET
MARKETGID
SUPERPOISK
RSCONTEXT
SPUTNIK
DIRECTST
GOOGADS
HOTLOGCH
LIVINETCH
BEGUNCH
UPDATE
SPLICEPROC
COOKREJCT
ZORKAFST
SEPARATEPROC
TERMINATE
DESTROY
```

Также после запуска бэкдор выполняет следующие действия:

- будучи запущенным с параметрами:

  ```
  /updatefile3
  /updatefile2
  /updatefile1
  ```

  бэкдор обновляет свой исполняемый файл, загружая обновление с сервера злоумышленника.
- Вызывая функцию "InternetClearAllPerSiteCookieDecisions", очищает содержимое ветви системного реестра:

  ```
  [HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\
  P3P\History]
  ```

- Создает ключи системного реестра:

```
[HKLM\Software\Microsoft\Netprotocol]
"UniqueNum" = ""

[HKCU\AppEvents\Schemes\Apps\Explorer\Navigating\.Current]
"(Default)" = ""

[HKCR\MIME\Database\Content Type\application/x-javascript]
"CLSID" = "{25336920-03F9-11cf-8FD0-00AA00686F13}"

[HKCR\MIME\Database\Content Type\text/javascript]
"CLSID" = "{25336920-03F9-11cf-8FD0-00AA00686F13}"
```