

*Дисциплина: МДК*

**Практическая работа**

# **«Изучение путей распространения и форм проявления компьютерных вирусов»**

**Выполнили:**

Нечаев А. Ю.

**Проверил:**

Возвахов Д.А.

Москва

2022

**Trojan-Banker.Win32.CliptoShuffler**

**Технические детали:**

Trojan-Spy:W32/Banker — большое семейство троянов для кражи данных. Варианты Banker пытаются украсть информацию о доступе к различным веб-сайтам онлайн-банкинга и платежных систем. Украденные данные включают учетные данные для входа в систему, пароли, PIN-коды и так далее. Украденная информация обычно загружается на веб-сайт хакера с помощью веб-формы.

Наиболее уязвимыми пользователями являются те, чьи логины и пароли для конфиденциальных онлайн-банковских или платежных счетов остаются неизменными при каждом сеансе входа в систему. По этой причине многие веб-сайты онлайн-банкинга меняют свои процессы безопасности, чтобы использовать одноразовые пароли, срок действия которых истекает после однократного использования.

**Деструктивная активность После запуска троянец выполняет следующие действия:**

*При инсталляции троянец копирует себя в корневой, системный и автозагрузочный каталоги Windows со следующими именами:*

%System%\load32.exe

%System%\vxdmgr32.exe

%User Profile%\Start Menu\Programs\Startup\rundllw.exe

%Windir%\dllreg.exe

***Затем регистрирует эти файлы в ключах автозапуска системного реестра:***

[HKLM\Software\Microsoft\Windows\CurrentVersion\Run]

"load32"="%System%\load32.exe"

[HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows]

"run"="%Windir%\dllreg.exe"

***Также троянец изменяет значение следующего ключа системного реестра:***

[HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon]

"Shell"="explorer.exe %Windir%\system32\vxdmgr32.exe"

***Оригинальное значение:***

"Shell"="explorer.exe"

При каждой следующей загрузке Windows автоматически запустит зараженные файлы.

***Также троянец создает следующий ключ в системном реестре:***

[HKLM\Software\SARS]

***В корневом каталоге Windows троянец создает следующий файл для захвата клавиатурного ввода пользователя:***

%Windir%\sock55.dll

***TrojanSpy.Win32.Banker.s собирает нажатия клавиш в окнах, заголовки которых содержат любое слово из следующего списка:***

@NetMan

banco

bank

barclays

credit report logon

e-gold Account

halifax

Hong Leong

hsbc

Login

LogOn

money

pay

punk

SignIn

SignOn

westpac

Yahoo! Mail

***Собранный клавиатурный ввод пользователя сохраняется в следующем файле:***

%Windir%\vxdload.txt

***Также троянец сохраняет всю информацию, находящуюся в буфере обмена в следующий файл:***

%Windir%\rundllx.sys

***Время от времени троянец отсылает созданные логи на email злоумышленника.***

**Рекомендации по удалению:**

1. ***Завершить следующие процессы и удалить соответствующие файлы:***

Orkut-SAC.exe

**Предупреждение:** вам необходимо удалить только файлы, контольные суммы которых, находятся в списке вредоносных. В вашей системе могут быть нужные файлы с такими же именами. **Рекомендуется** использовать **Утилиту для удаления Trojan-Spy.Win32.Banker.ark** для безопасного решения проблемы.

1. ***Удалите следующие папки:***

no information

1. ***Удалите следующие ключи и\или значения ключей реестра:***

no information

**Предупреждение:** Если указаны значения ключей реестра, вы должны удалить только указанные значения и оставить сами ключи нетронутыми. **Рекомендуется** использовать **Утилиту для удаления Trojan-Spy.Win32.Banker.ark**для безопасного решения проблемы.

Как предотвратить заражение рекламным ПО? **Рекомендуется** использовать **Adguard**

1. ***Сбросить настройки браузеров***

Trojan-Spy.Win32.Banker.ark иногда может влиять на настройки вашего браузера, например, подменять поиск и домашнюю страницу. Мы рекомендуем вам использовать бесплатную функцию "Сбросить настройки браузеров" в "Инструментах" в программе **Spyhunter Remediation Tool** для сброса настроек всех браузеров разом. Учтите, что перед этим вам надо удалить все файлы, папки и ключи реестра, принадлежащие **Trojan-Spy.Win32.Banker.ark.** Для сброса настроек браузеров вручную используйте данную инструкцию:

Для **Internet Explorer**

Если вы используете Windows XP, кликните Пуск, и Открыть. Введите следующее в поле *Открыть* без кавычек и нажмите Enter: "inetcpl.cpl".

Если вы используете Windows 7 или Windows Vista, кликните Пуск. Введите следующее в поле *Искать* без кавычек и нажмите Enter: "inetcpl.cpl".

Выберите вкладку *Дополнительно*

Под Сброс параметров браузера Internet Explorer, кликните Сброс. И нажмите Сброс ещё раз в открывшемся окне.

Выберите галочку *Удалить* личные настройки для удаления истории, восстановления поиска и домашней страницы.

После того как Internet Explorer завершит сброс, кликните *Закрыть* в диалоговом окне.

**Предупреждение:** В случае если это не сработает используйте бесплатную опцию *Сбросить* настройки браузеров в *Инструменты* в программе **Spyhunter Remediation Tool**.

Для **Google Chrome**

Найдите папку установки Google Chrome по адресу: C:\Users\"имя пользователя"\AppData\Local\Google\Chrome\Application\User Data.

В папке *User Data*, найдите файл *Default*и переименуйте его в *DefaultBackup*.

Запустите *Google Chrome* и будет создан новый файл *Default*.

Настройки *Google Chrome* сброшены

**Предупреждение:** В случае если это не сработает используйте бесплатную опцию Сбросить настройки браузеров в Инструменты в программе **Spyhunter Remediation Tool**.

Для **Mozilla Firefox**

Откройте *Firefox*

В меню выберите *Помощь* > *Информация для решения проблем*.

Кликните кнопку *Сбросить Firefox*.

После того, как *Firefox* завершит, он покажет окно и создаст папку на рабочем столе. Нажмите *Завершить*.

Предупреждение: Так вы потеряете ваши пароли! Рекомендуем использовать бесплатную опцию Сбросить настройки браузеров в Инструменты в программе **Spyhunter Remediation Tool**.

**Virus.Win32.Nimnul**

**Технические детали:**

Virus.Nimnul.Win32.2  – вирус, заражающий exe, dll и Html файлы, а также  открывающий  злоумышленнику удаленный доступ к зараженной машине. Является приложением Windows (EXE файл). размер ~ 65 Кбайт.

**Деструктивная активность После запуска троянец выполняет следующие действия:**

1. Вирус  создает свои  копии на  всех доступных для записи дисках, включая сетевые и съемные, для этого он  копирует свое тело в папку "<диск>:\Recycler\".  
   В корне зараженного диска создается сопутствующий файл  autorun.inf, который позволит вирусу запускаться каждый раз, когда пользователь открывает зараженный диск при помощи программы "Проводник".
2. Вирус заражает exe и dll файлы, для этого он расширяет последнюю секцию заражаемого файла и дописывает туда своё тело. После чего изменяет точку входа, чтобы она указывала на вирусное тело.
3. Вирус заражает html файлы, для этого он дописывает в конец файла Java-скрипт  содержащий тело вируса в HEX кодах, а также команды, которые извлекают его тело во временную папку и запускают на выполнение. Таким образом, при каждом запуске html файла будет создаваться, и запускаться копия вируса.

***Техническое описание***

После запуска  вирус создает папку microsof, которая может располагаться  в одной из следующих папок

%System%  
%WinDir%  
%Temp%  
%HOMEPATH%  
%HOMEDRIVE%  
%APPDATA%

После чего копирует туда свое тело под одним из случайных имён.

***Например:  
 c:\program files\microsoft\watermark.exe***

Для автозапуска, при каждом старте системы, вирус добавляет ключ реестра:

***[HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\]  
Userinit ="c:\program files\microsoft\watermark.exe"***   (Путь к телу вируса и имя вируса могут принимать разные значения)

В одной из папок создается конфигурационный файл вируса, под именем dmlconf.dat

***Например:  
C:\WINDOWS\system32\dmlconf.dat***

После запуска вирус запускает браузер, и внедряется в его адресное пространство. Также вирус внедряется в память других системных процессов, таких как lsass.exe, svchost.exe и т.д.

Наличие зараженных процессов в системе позволяет вирусу инфицировать exe и html файлы, а также противодействовать попыткам удалить его файлы из системы, или изменить записи в реестре.

Для контроля  своего процесса вирус создает уникальный идентификатор Mutex с именем  “\_\_PDH\_PLA\_MUTEX\_\_”.

***Деструктивные возможности***

После запуска вирус проверяет наличие сети Internet, обращаясь к серверу google.com, после чего создает соединение с сервером злоумышленников для получения команд управления.

Вирус, по команде с удаленного сервера, может загружать на зараженный компьютер файлы и запускать их на выполнение, таким образом на компьютере может оказаться большое количество разнообразного вредоносного ПО, такого как Backdoor , троянские программы и т.п.

**Рекомендации по удалению:**

1. Если ваш компьютер не был защищен антивирусом и оказался заражен данной вредоносной программой, то для её удаления необходимо выполнить следующие действия:
2. При помощи Диспетчера задач завершить процесс установленного по умолчанию браузера.
3. Восстановить значение ключа системного реестра:
4. [HKLM/Software/Microsoft/Windows NT/CurrentVersion/Winlogon]  
   "Userinit" = "userinit.exe"
5. Удалить файлы:
6. %Program Files%MicrosoftDesktopLayer.exe  
   %Temp%/svchost.exe  
   имя зараженного диска:/Recycler  
   имя зараженного диска:/autorun.inf
7. Удалить оригинальный файл вредоноса (его расположение на зараженном компьютере зависит от способа, которым программа попала на компьютер).
8. Не запускать EXE, HTM файлы и не перезагружать компьютер до полной проверки зараженного компьютера антивирусом.
9. Очистить каталог Temporary Internet Files.
10. Произвести полную проверку компьютера Антивирусом Касперского с обновленными антивирусными базами ([скачать пробную версию](http://www.kaspersky.ru/trials)).

**Trojan.Win32.Neurevt**

**Технические детали:**

Trojan.Win32.Neurevt представляет из себя многофункциональный троянец, написанный на языке C++. Троянец известен также под названием Betabot.

Троянец использует руткит-технологии для скрытия своего присутствия в системе, внедряет свой код во все запущенные процессы, блокирует работу некоторых антивирусов, может распространяться через флеш-накопители. Также троянец может отслеживать и блокировать установку других распространенных троянских программ, проводить DDoS-атаки, перехватывать и подменять пользовательский трафик, перехватывать пароли из приложений, работающих по протоколам FTP, POP3 и SSH, подменять DNS-запросы, искать и отправлять злоумышленнику определенные файлы на зараженном компьютере, создавать прокси-сервер, работающий по протоколу SOCKS.

**Деструктивная активность После запуска троянец выполняет следующие действия:**

Эта угроза использует случайное имя файла. Он обнаружен в папке с частично случайным именем - *%ProgramFiles%\common files\*<случайная фраза>*.{2227a280-3aea-1069-a2de-08002b30309d}*.

***Например:***

* [%ProgramFiles%](https://www.microsoft.com/en-us/wdsi/help/folder-variables#programfiles) \общие файлы\бета-бот.{2227a280-3aea-1069-a2de-08002b30309d}\kbqiypzyt.exe
* [%ProgramFiles%](https://www.microsoft.com/en-us/wdsi/help/folder-variables#programfiles) \общие файлы \ браузер chrome.{2227a280-3aea-1069-a2de-08002b30309d}\auaucdlve.exe

Он также создает следующие записи в реестре, чтобы автоматически запускаться при каждом запуске Windows:

В подразделе: *HKLM \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Run*  
Задает значение: "<случайная фраза>"  
С данными: "*%ProgramFiles%\общие файлы\*<случайная фраза>*.{2227a280-3aea-1069-a2de-08002b30309d} \*<имя вредоносного файла>*.exe*"

***Например:***

***В подразделе:***HKLM \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Run ***Задает значение:*** "Бета-бот" ***с данными:*** "%ProgramFiles% \общие файлы \ бета-бот.{2227a280-3aea-1069-a2de-08002b30309d} \kbqiypzyt.exe "

***В подразделе***: HKLM \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Run ***Задает значение:*** "Браузер Chrome" ***с данными:*** "%ProgramFiles% \общие файлы \ браузер Chrome.{2227a280-3aea-1069-a2de-08002b30309d}\auaucdlve.exe "

***В процессе установки также создается следующая запись реестра:***

***в подразделе***: HKCU \ Software \ Win7zip ***Задает значение:*** "Uuid" ***с данными:*** "<случайный байт-код>"

***Например:***

***в подразделе:***HKCU \ Software \ Win7zip  
***Задает значение:*** "Uuid" ***с данными:*** "u^â..ny".

***Изменяет настройки вашего компьютера***

Этот троянец скрывает файлы и папки с атрибутом "*system*", изменяя следующую запись реестра:

***В подразделе:*** *HKCU \ Software \ Microsoft \ Windows \ CurrentVersion\ Explorer\Advanced*  
Задает значение: "*ShowSuperHidden*"  
с данными: "*0*"

***Предотвращает запуск некоторых процессов безопасности***

***Этот троянец предотвращает запуск некоторых процессов безопасности, добавляя следующие записи реестра:***

***В подразделе:*** *HKLM \ SOFTWARE \ Microsoft \ Windows NT \ CurrentVersion\Выполнение файла изображения Options\rstrui.exe*  
***Задает значение:*** "*Debugger*"  
***с данными:*** "<случайные символы> \_*.exe*"

***В подразделе:*** *HKLM \ SOFTWARE \ Microsoft \ Windows NT \ CurrentVersion\Выполнение файла изображения Options\hijackthis.exe*  
***Задает значение:*** "*Debugger*"  
***с данными:*** "<случайные символы> \_*.exe*"

***В подразделе:*** *HKLM \ SOFTWARE \ Microsoft \ Windows NT \ CurrentVersion\Выполнение файла изображения Options\spybotsd.exe*  
***Задает значение:*** "*Debugger*"  
***с данными:*** "<случайные символы> \_*.exe*"

***В подразделе:*** *HKLM \ SOFTWARE \ Microsoft \ Windows NT \ CurrentVersion\Выполнение файла изображения Options\housecalllauncher.exe*  
***Задает значение:*** "*Debugger*"  
***с данными:*** "<случайные символы> \_*.exe*"

***Например:***

***В подразделе:*** *HKLM \ SOFTWARE \ Microsoft \ Windows NT \ CurrentVersion\Выполнение файла изображения Options\rstrui.exe*  
***Задает значение:*** "*Debugger*"  
***с данными:*** "dwrdsye\_.exe "

В подразделе: *HKLM \ SOFTWARE \ Microsoft \ Windows NT \ CurrentVersion\Выполнение файла изображения Options\hijackthis.exe*  
***Устанавливает значение:*** "*Отладчик*"  
***с данными:*** "rj\_.exe "

В подразделе: *HKLM \ SOFTWARE \ Microsoft \ Windows NT \ CurrentVersion\Выполнение файла изображения Options\spybotsd.exe*  
***Устанавливает значение:*** "*Отладчик*"  
***с данными:*** "cxsrjn\_.exe "

В подразделе: *HKLM \ SOFTWARE \ Microsoft \ Windows NT \ CurrentVersion\Выполнение файла изображения Options\housecalllauncher.exe*  
***Задает значение:*** "*Debugger*"  
***с данными:*** "*eivm\_.exe* "

**Отключает защищенный режим в Internet Explorer**

***Этот троянец отключает режим защиты в Internet Explorer во всех зонах, изменяя следующие записи реестра:***

***В подразделе:*** *HKCU \ Software \ Microsoft \ Windows \ CurrentVersion \ Настройки Интернета \ Зоны \ 1*  
***Задает значение:*** "*2500*"  
***с данными:*** "*3*"

***В подразделе:*** *HKCU \ Software \ Microsoft \ Windows \ CurrentVersion \ Настройки Интернета \ Зоны \ 2*  
***Задает значение:*** "*2500*"  
***с данными:*** "*3*"

***В подразделе:*** *HKCU \ Software \ Microsoft \ Windows \ CurrentVersion \ Настройки Интернета \ Зоны \ 3*  
***Задает значение:*** "*2500*"  
***с данными:*** "*3*"

***В подразделе:*** *HKCU \ Software \ Microsoft \ Windows \ CurrentVersion \ Настройки Интернета \ Зоны \ 4*  
***Задает значение:*** "*2500*"  
***с данными:*** "*3*"

**Крадет данные компьютера и учетной записи**

***Этот троянец крадет любые сохраненные имена пользователей и пароли, серверы и подключения к портам из следующих FTP-программ, если они установлены на вашем ПК:***

* *CoreFTP*
* *FileZilla*
* *FlashFXP*
* *FTP Commander*
* *Шпатлевка*
* *SmartFTP*
* *WinSCP*

Он также может украсть данные вашей учетной записи и список контактов для Skype.

***Он также может украсть информацию о вашем компьютере, например:***

* Операционная система
* Пользователь, вошедший в систему в данный момент
* Программное обеспечение, установленное на вашем компьютере, особенно программное обеспечение безопасности

**Позволяет использовать бэкдор для доступа и управления**

Этот троянец может подключаться к удаленным серверам, чтобы предоставить злоумышленнику доступ к вашему компьютеру. ***Он пытается подключиться к следующим серверам:***

* *strike-file-hosting.us*
* *188.190.99.224*

***После подключения злоумышленник может выполнить следующие действия с вашим компьютером:***

* Загружайте и запускайте произвольные файлы
* Загрузить файлы
* Отправляет украденные данные
* Распространяется через съемные диски
* Запуск или остановка программ
* Удаление файлов

**Рекомендации по удалению:**

1. Откройте главное меню операционной системы и запустите панель управления. В открывшемся окне выберите компонент «Установка и удаление программ». В списке установленных программ найдите запись "Trojan.Win32", выделите и удалите эту программу. Удаление производится обычным способом, следуйте инструкциям, которые будут появляться на экране. Завершив удаление программы, перезагрузите компьютер.
2. Закройте все запущенные программы. Остановите процесс "Trojan.Win32", для этого запустите «Диспетчер задач» (комбинацией клавиш Ctrl+Alt+Delete или правой кнопкой на панели задач). В списке запущенных процессов найдите и выберите процесс, который необходимо остановить, затем щелкните кнопку «Завершить процесс». Закройте «Диспетчер задач».
3. Воспользовавшись системой поиска операционной системы или файловым менеджером, найдите и удалите следующие файлы: windivx.dll, vipextqtr.dll, stream32a.dll, ecxwp.dll. Также эти файлы можно просто переименовать, дав им имена bad1.dll, bad2.dll и т.д. Если переименовать файлы не удается, сделайте это, перезагрузив операционную систему в безопасном режиме.
4. Откройте папку "C:\Program Files", найдите и удалите в ней папку "VirusProtect 3.8". Если удалить папку не удается, перезапустите компьютер в безопасном режиме и повторить попытку. Для удаления не удаляемых папок и файлов можно также воспользоваться специальными программами, например Unlocker. Перезагрузите компьютер.
5. Для предотвращения заражения компьютера вирусом Win32 в будущем установите лицензионную программу антивирусной защиты и регулярно обновляйте ее базу. Так вы защите свой компьютер не только от данного вируса, но и от более вредоносных программ, например, крадущих пароли, личные данные и т.д.

**Контрольные вопросы**

1. Взять описание работы компьютерных вирусов можно с данных сайтов:

* https://threats.kaspersky.com/ru/class/Trojan-Banker/[www.nkj.ru](http://www.nkj.ru)
* <https://threats.kaspersky.com/ru/threat/Trojan.Win32.Neurevt/>
* <https://threats.kaspersky.com/ru/threat/Virus.Win32.Nimnul/>

1. Интернет и носители информации – главные распространители компьютерных вирусов
2. Осложнение загрузки ОС, медленная работа ПК, исчезновение файлов и каталогов или искажение их содержимого и прекращение работы ранее успешно функционировавших программ.
3. Наиболее незаметными проявлениями компьютерных вирусов для пользователя являются использование компьютера пользователя для организации ДДОС- аттак, фишинги, майнеры.