**Лабораторная работа №1 Изучение путей распространения и форм проявления компьютерных вирусов**

**Цель работы и содержание:** изучить пути распространения и формы проявления компьютерных вирусов.

**Сайт -** [**Android.Joker**](https://vms.drweb.ru/search/?q=Android.Joker&lng=ru).

Среди угроз, выявленных в каталоге Google Play в 2021 году, было множество троянов, принадлежащих к семейству [**Android.Joker**](https://vms.drweb.ru/search/?q=Android.Joker&lng=ru). Они опасны тем, что способны загружать и исполнять произвольный код, а также автоматически подписывать пользователей на платные мобильные услуги. Эти трояны распространялись под видом самых разных приложений ― фото- и видеоредакторов, музыкальных плееров, мессенджеров, программ для работы с документами и заботы о здоровье, переводчиков, утилит для оптимизации работы системы и других. При этом они выполняли заявленные функции, чтобы потенциальные жертвы не заподозрили в них угрозу. В течение года вирусные аналитики «Доктор Веб» выявили в Google Play более 40 неизвестных ранее модификаций таких вредоносных приложений, число установок которых превысило 1 250 000.

**Процесс:**

Использует следующие алгоритмы для шифрования данных:

* AES-CBC-PKCS5Padding
* DES-CBC-PKCS5Padding

Использует следующие алгоритмы для расшифровки данных:

* AES-CBC-PKCS5Padding

Осуществляет доступ к приватному интерфейсу ITelephony.

Получает информацию о сети.

Получает информацию о телефоне (номер, IMEI и т. д.).

Получает информацию об установленных приложениях.

Получает информацию о запущенных приложениях.

Получает информацию о привязанных к устройству аккаунтах (Google, Facebook и т. д.).

Отрисовывает собственные окна поверх других приложений.

Перехватывает уведомления.

Содержит Play Store Frosting.

**Рекомендации по лечению**

1. Если мобильное устройство функционирует в штатном режиме, загрузите и установите на него бесплатный антивирусный продукт [Dr.Web для Android *Light*](hhttps://free.drweb.ru/drweb+android+light/). Выполните полную проверку системы и используйте рекомендации по нейтрализации обнаруженных угроз.
2. Если мобильное устройство заблокировано троянцем-вымогателем семейства Android.Locker (на экране отображается обвинение в нарушении закона, требование выплаты определенной денежной суммы или иное сообщение, мешающее нормальной работе с устройством), выполните следующие действия:
   * загрузите свой смартфон или планшет в безопасном режиме (в зависимости от версии операционной системы и особенностей конкретного мобильного устройства эта процедура может быть выполнена различными способами; обратитесь за уточнением к инструкции, поставляемой вместе с приобретенным аппаратом, или напрямую к его производителю);
   * после активации безопасного режима установите на зараженное устройство бесплатный антивирусный продукт [Dr.Web для Android *Light*](https://free.drweb.ru/drweb+android+light/) и произведите полную проверку системы, выполнив рекомендации по нейтрализации обнаруженных угроз;
   * выключите устройство и включите его в обычном режиме.

**Tool.SilentInstaller**

Детектирование программной платформы [VirtualApp](https://github.com/asLody/VirtualApp) и ее модификаций. Она создает виртуальную среду для выполнения приложений и плагинов без их непосредственной установки на целевых устройствах под управлением ОС Android. Этот метод может использоваться для запуска произвольного кода во вредоносных целях, поэтому указанная платформа является потенциально опасной.

**Процесс:**

Ищет следующие окна

* ClassName: '18467-41' WindowName: ''

Создает и запускает на исполнение

* '%TEMP%\sib8058.tmp\1\do\_1.exe' /s

Запускает на исполнение

* '%WINDIR%\syswow64\cscript.exe' s1.vbs //e:vbscript //NOLOGO

**Рекомендации по лечению**

1. В случае если операционная система способна загрузиться (в штатном режиме или режиме защиты от сбоев), скачайте лечащую утилиту [Dr.Web CureIt!](https://free.drweb.ru/cureit/) и выполните с ее помощью полную проверку вашего компьютера, а также используемых вами переносных носителей информации.
2. Если загрузка операционной системы невозможна, измените настройки BIOS вашего компьютера, чтобы обеспечить возможность загрузки ПК с компакт-диска или USB-накопителя. Скачайте образ аварийного диска восстановления системы [Dr.Web® LiveDisk](https://free.drweb.ru/aid_admin/) или утилиту записи [Dr.Web® LiveDisk](https://free.drweb.ru/aid_admin/) на USB-накопитель, подготовьте соответствующий носитель. Загрузив компьютер с использованием данного носителя, выполните его полную проверку и лечение обнаруженных угроз.

**Сайт** - <https://vms.drweb.ru/virus/?i=25556572>

Это вредоносное программное обеспечение, которое маскирует свое истинное назначение. При этом, в отличие от вируса, троян не способен самостоятельно дублировать или заражать файлы. Чтобы проникнуть на устройство жертвы, данное вредоносное ПО использует другие средства, такие как скрытая загрузка, использование уязвимостей, загрузка через другой вредоносный код или методы социальной инженерии.

**Процесс:**

Подключается к

* 'fu###ujjul.net':80
* 'st####stitibo.org':80
* 'li####tiyyyul.net':80
* 'gu####na49org.org':80
* 'st###nuytyt.org':80
* 'yo####umenia5.org':80

TCP

Запросы HTTP POST

* http://fu###ujjul.net/
* http://st####stitibo.org/
* http://li####tiyyyul.net/
* http://gu####na49org.org/
* http://st###nuytyt.org/
* http://yo####umenia5.org/

UDP

* DNS ASK fu###ujjul.net
* DNS ASK st####stitibo.org
* DNS ASK li####tiyyyul.net
* DNS ASK bu####tu44org.org
* DNS ASK nv###kuluir.net
* DNS ASK gu####na49org.org
* DNS ASK hu####dulinu.net
* DNS ASK st###nuytyt.org
* DNS ASK nu###tnulo.me
* DNS ASK yo####umenia5.org
* DNS ASK gu####iimnstra.net

Троян может несколько дней находиться в режиме ожидания, не выполняя никаких действий. Антивирусы могут не обнаруживать его в это время, так как подозрительное поведение отсутствует.

Рано или поздно троян соединяется с сервером, точнее с центром управления. Откуда получает некоторые конфигурационные данные: список запасных серверов (IP-адреса), список адресов для загрузки, команды на выполнение.

Троян загружает другие вирусы из сети и запускает их. При этом может анализироваться состояние ПК — наличие антивируса, мощность процессора, видеокарты. Вирусы загружаются те, которые вероятно не будут обнаружены.

**Рекомендации по лечению**

1. В случае если операционная система способна загрузиться (в штатном режиме или режиме защиты от сбоев), скачайте лечащую утилиту [Dr.Web CureIt!](https://free.drweb.ru/cureit/) и выполните с ее помощью полную проверку вашего компьютера, а также используемых вами переносных носителей информации.
2. Если загрузка операционной системы невозможна, измените настройки BIOS вашего компьютера, чтобы обеспечить возможность загрузки ПК с компакт-диска или USB-накопителя. Скачайте образ аварийного диска восстановления системы [Dr.Web® LiveDisk](https://free.drweb.ru/aid_admin/) или утилиту записи [Dr.Web® LiveDisk](https://free.drweb.ru/aid_admin/) на USB-накопитель, подготовьте соответствующий носитель. Загрузив компьютер с использованием данного носителя, выполните его полную проверку и лечение обнаруженных угроз.

**Сайт -** <https://vms.drweb.ru/virus/?i=25556594>

**Процесс:**

Подменяет следующие исполняемые файлы

* <Полный путь к файлу>

Самоперемещается

* из <Полный путь к файлу> в <Текущая директория>\old\_<Имя файла>.exe

Самоудаляется

**Рекомендации по лечению**

1. В случае если операционная система способна загрузиться (в штатном режиме или режиме защиты от сбоев), скачайте лечащую утилиту [Dr.Web CureIt!](https://free.drweb.ru/cureit/) и выполните с ее помощью полную проверку вашего компьютера, а также используемых вами переносных носителей информации.
2. Если загрузка операционной системы невозможна, измените настройки BIOS вашего компьютера, чтобы обеспечить возможность загрузки ПК с компакт-диска или USB-накопителя. Скачайте образ аварийного диска восстановления системы [Dr.Web® LiveDisk](https://free.drweb.ru/aid_admin/) или утилиту записи [Dr.Web® LiveDisk](https://free.drweb.ru/aid_admin/) на USB-накопитель, подготовьте соответствующий носитель. Загрузив компьютер с использованием данного носителя, выполните его полную проверку и лечение обнаруженных угроз.

**Контрольные вопросы**

**1.** Где можно взять описание работы компьютерных вирусов (конкретные примеры)?

<https://vms.drweb.ru/search/>

<https://teralex.ru/bezrubriki/kompyuternye-virusy-tipy-vidy-puti-zarazheniya.html>

[htt http://www.securelist.com/ru/descriptions http://www.kaspersky.ru/rss/technews http://www.securitylab.ru/\_Services/Export/RSS/ http://www.viruslist.com/ru/rss/latestvirusdescriptions http://www.viruslist.com/ru/rss/virusalerts http://www.viruslist.com/ru/rss/latestnews http://news.drweb.com/list/?c=10 http://www.kaspersky.com/viruswatch3ps://www.virustotal.com/gui/home/upload](https://www.virustotal.com/gui/home/upload)

**2.** Какие есть пути распространения компьютерных вирусов ?

* **Письма со спамом** - Авторы вредоносных программ часто пытаются обманным умыслом скачать вредоносные файлы. Это может быть письмо с вложенным файлом, который описывается как уведомление о доставке, возврат налогового платежа или счет по купленному билету. В письме может быть сказано, что необходимо открыть вложение, чтобы получить отправление или деньги.
* **Вредоносные Office макрос** - Microsoft Office включает в себя мощный язык сценариев, позволяющий разработчикам создавать дополнительные инструменты, которые помогут вам работать продуктивнее. К сожалению, злоумышленники также могут использовать этот язык для создания вредоносных сценариев, которые устанавливают вредоносные программы или делают другие плохие вещи.
* **Зараженные съемные носители** - Многие вредоносные программы распространяются, заражая съемные носители, такие как USB-устройства флэш-памяти или внешние жесткие диски. Вредоносная программа может автоматически установиться при подключении зараженного носителя к компьютеру
* **Вместе с другим программным обеспечением** - Некоторые вредоносные программы могут устанавливаться одновременно с другими скачанными программами. К таким программам относится программное обеспечение со сторонних веб-сайтов или файлы, передаваемые через одноранговые сети.
* **Взломанные или скомпрометированные веб-страницы** - Вредоносные программы могут использовать известные программные уязвимости для заражения компьютера. Уязвимость — это брешь в программном обеспечении, через которую вредоносные программы могут получить доступ к компьютеру.
* **Другие вредоносные программы** - Некоторые типы вредоносных программ могут загружать на компьютер другие угрозы. После установки этих угроз на компьютере они продолжат загружать дополнительные угрозы.

**3.** Какие есть формы проявления компьютерных вирусов ?

* **Черви — Worm.** Червь – программа, которая делает копии самой себя. Ее вред заключается в захламлении компьютера, из-за чего он начинает работать медленнее. Отличительной особенностью червя является то, что он не может стать частью другой безвредной программы.
* **Вирусы-маскировщики — Rootkit**. Эти вирусы используются для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами. Rootkit'ы также могут модифицировать операционную систему на компьютере и заменять основные ее функции, чтобы скрыть свое собственное присутствие и действия, которые предпринимает злоумышленник на зараженном компьютере.
* **Вирусы – шпионы — Spyware.** Шпионы собирают информацию о действиях и поведении пользователя. В основном их интересует информация — адреса, пароли, данные кредитных карт).
* **Зомби — Zombie**. Зомби позволяют злоумышленнику управлять компьютером пользователя. Компьютеры – зомби могут быть объединены в сеть —бот-нет) и использоваться для массовой атаки на сайты или рассылки спама. Пользователь может даже не догадываться, что его компьютер зомбирован и используется злоумышленником.
* **Рекламные вирусы — Adware**. Программы-рекламы, без ведома пользователей встраиваются в различное программное обеспечение с целью демонстрации рекламных объявлений. Как правило, программы-рекламы встроены в программное обеспечение, распространяющееся бесплатно. Реклама располагается в рабочем интерфейсе. Зачастую данные программы также собирают и переправляют своему разработчику персональную информацию о пользователе.
* **Вирусы – блокировщики — Winlock**. Такие программы блокирует пользователю доступ к операционной системе. При загрузке компьютера появляется окно,  в котором пользователя обвиняют в скачивании нелицензионного контента или нарушении авторских прав.  И под угрозой полного удаления всех данных с компьютера требуют отослать смс на номер телефона или пополнить его счет. Естественно, после перевода денег на счет злоумышленника, баннер никуда не пропадает.
* **Троянские вирусы — Trojan**. Троянская программа является самым опасным типом вирусов, так как она маскируется в других безвредных программах. И до того момента как пользователь не запустит эту самую безвредную программу,  троян не несет никакой опасности и обнаружить его нелегко. Троянская программа может нанести различный ущерб для компьютера. В основном трояны используются для кражи, изменения или удаления личных данных пользователя. Отличительной особенностью вируса-трояна является то, что он не может самостоятельно размножаться.

**4.** Какие формы проявления компьютерных вирусов наиболее незаметны для пользователя?

Вирус загрузочного сектора  
Вирус перезаписи  
Полиморфный вирус

Червь

Троян

**Соцкова К.А., Зайцева А.С, Зверькова Е.А.**