Scientific and Practical Cyber Security Journal (SPCSJ) 2(1):60-62
Scientific Cyber Security Association (SCSA), 2018 ISSN: 2587-4667

VIRUSES. EXECUTING PRINCIPLES AND METHODS OF SELF-SECURITY

B.Horbatenko, V.Stopin
Kharkiv National University of Radio Electronics (NURE), Kharkiv, Ukraine

ABSTRACT. Types of viruses that mainly spread in the Internet are proposed in this paper. There we tried to generalize technical experience and give some practical recommendations.
This paper will be useful as for newbie users as for advanced users. It is said about most common virus programs, how they work and methods how to stay secure.

Аннотация. В данной статье представлены основные квалификации вирусов, которые наиболее распространены в глобальной сети Интернет. Мы постарались обобщить технический опыт по данной теме и сделать упор на практические рекомендации.
Данная статья предназначена как для опытных пользователей, так и для новичков. В ней говориться о наиболее распространенных вирусах, принципом работы и методами, как остаться защищенным.

KEYWORDS: Windows, Virus, Cybersecurity, Trojan, RAT, Winlocker, Keylogger, Worm, Stiller.

Вирусные эпидемии теперь могут встречаться не только в реальной жизни, а и в виртуальной. Время, когда компьютерные вирусы были безобидными – бесследно прошло. Вред от вирусов не знает пределов, а ущерб, который они могут принести вашей системе, поражает воображение. Создание и распространение вирусов во многих странах преследуется законом как уголовное преступление. Ваш компьютер может быть заражен в любое время и степень вреда от вируса, зависит исключительно от его типа.
Компьютерные вирусы имеют способность абсолютно “бесшумно” внедряться в систему и таким же образом распространятся. Заразить компьютер можно различными способами, например, перейти по ссылке, пришедшей вам на почту или открыть картинку, замаскированную под вирус. Вирусная эпидемия может в считанные дни или часы охватить крупный вычислительный центр (а то и несколько центров), полностью парализовав его работу. Примером тому является нашумевший вирус под названием Petya, который парализовал работу множества важных ресурсов государственного и коммерческого сектора Украины. Издержки от этого заражения исчисляются миллионами долларов.
Существует множество типов вирусов, рассмотрим основные из них:

Winlocker – данный тип вирусов блокирует работу операционной системы, обычно эта блокировка заключается в покрытии экрана рабочего стола каким-то слоем, который не позволяет взаимодействовать с папками и файлами в системе, помимо этого деактивируются вспомогательные средства в виде диспетчера задач и других вспомогательных средств. Для разблокировки компьютера вирус вымогают средства. Данный тип вирусов нельзя отнести к особо опасным, большинство из них выключается посредством безопасного режима или в режиме командной строки, однако существует ряд модификаций этого вируса, которые уже несут в себе намного значительный вред для системы пользователя.

Cryptor – является одной из модификаций winlocker. Предназначение этого вируса заключается в шифровании всех данных на компьютере. Зашифровав все файлы на компьютере пользователя, вирус вымогает с пользователя деньги для дешифрования и разблокировки компьютера. Оплата за ключ для дешифрования и разблокировки составляет от 500 долларов и выше. Целью мошенников, распространяющих вирусов, являются компьютеры с коммерческими, рабочими или личными данными. В основном упор делается на состоятельных личностей или учреждения. Примером данного типа вирусов является вирус-вымогатель Petya. По некоторым источникам, данный вирус нанес ущерб в более чем 60 странах мира, на сумму, превышающую восемь миллиардов долларов. Избавиться от хорошего криптора достаточно сложно.

Trojan – это программное обеспечение, которое позволяет получить доступ к удаленному компьютерному средству, позволяет получать различные данные о системе жертвы, управлять ею, пересылать или получать данные. Делятся на 3 типа: Remote Administrator Tool (RAT), Keylogger, Stiller.

Remote administrator tool (RAT) – данный тип вирусов предназначен в первую очередь для удаленного управления компьютером пользователя. Данный тип по праву можно называть программным обеспечением двойного назначения. Хорошими примерами одобренных и не считающимся вирусами RAT являются: TeamViever, Oscelestial, Remmina, Radmin. Перечисленные программы не считаются вирусами по той причине, что они позволяют иметь удаленный контроль только при согласии двух сторон, однако при некоторых модификациях, злоумышленник может и в одностороннем порядке настроить удаленное управление при помощи данных программных средств. По итогу, данный тип вирусов, позволяют проводить некоторые скрытые процессы от владельца компьютера, например, просматривать его экран в реальном времени, управлять компьютерным средством, скачивать и загружать данные на компьютер жертвы, прослушивать микрофон жертвы и многое другое. Для осуществления атаки и внедрения на компьютер, достаточно, чтобы жертва запустила файл. Исполняемый файл можно поместить в различные форматы файлов, например, в .jpeg или .doc.
В основе большинства вирусов используются так называемые шифровщики или крипторы. Это своеобразные механизмы, которые используются для запутывания антивирусов. Они изменяют поведенческие факторы программного средства и делают его незаметным для большинства или всех антивирусных средств, и позволяет беспрепятственно проникнуть на компьютер.

Keylogger & Stiller – данные два типа вирусов объединены в одно по той причине, что в большинстве случаев они являются одним целым вирусом. Принцип их работы заключается в краже конфиденциальных данных пользователей, например, паролей, учетных данных и так далее. Помимо этого, данный тип вирусов считывает все введенные значения с клавиатуры пользователей, вплоть до нажатия сочетаний клавиш. Таким образом, злоумышленник может заполучить данные от ваших кредитных карт или иных ресурсов, которые вы вводите с клавиатуры. Настоятельно не рекомендуется хранить пароли в браузерах, все пароли хранятся в хранилищах браузера, а данный тип вирусов их оттуда легко скачивает и передает злоумышленнику.

Worm – вид вируса, который самостоятельно распространяется в сети. В большинстве случаев они распространяются при помощи бреши (уязвимости) в системе безопасности той или иной операционной системы. Достаточно заразить один компьютер в сети, а дальнейшее его распространение будет проходить автономно.

Принято считать, что антивирусы могут защитить от вирусов. Однако это утверждение является частично неверным. Антивирусы работают по двум основным алгоритмам – структурный и поведенческий анализ. От структурной проверки можно защититься с помощью криптора, который упоминался ранее. Поведенческий анализ можно обойти правильным написанием функций, который не вызовет подозрений у алгоритмов антивирусного средства. Таким образом нельзя утверждать о предоставлении полноценной безопасности антивирусом.

Помочь в борьбе с вирусами может переход на Linux-подобные системы, так как достаточно сложно найти вирусы, разработанные исключительно под данную версию операционной системы. Однако это не значит, что вирусов под Linux нет, их просто меньше. Не стоит терять бдительность.

Firewall (Анализ сетевой активности) может значительно помочь в борьбе с вирусами, использующими сеть Интернет для своей работы, например, Remote Administrator Tool (RAT). Грамотно настроенный Firewall позволит почти полностью исключить всяческие сетевые атаки и манипуляции извне с вашим компьютером. При помощи Firewall, можно посмотреть, какие приложения и из каких стран используют выход в интернет, с чем хотят связаться.

Сканирование вашей системы различными средствами (HitmanPro, Avz и другие) смогут предотвратить деятельность вирусов на вашем компьютерном средстве. Да, это не всегда лучший метод борьбы с опасными вирусами, однако бывают исключения из правил и подобные средства оказывают значительную помощь при лечении вашего компьютера от заражения.

Используйте виртуальную машину для открытия подозрительных ссылок и файлов. Виртуальная машина создает контейнер внутри вашей операционной системы, который позволяет безопасно взаимодействовать с различными файлами и данными. Если файл является зараженным, то все его пагубные действия остаются внутри этого контейнера.
Большинство угроз поджидает пользователей при переходе по неизвестной ссылке и запуске файлов. В коммерческих и государственных учреждениях идет большой документооборот и очень часто злоумышленники используют этот фактор для внедрения своих вирусов. Для предотвращения заражения компьютера вирусом можно использовать рекомендации, приведенные выше. Несомненно, это может незначительно замедлить и усложнить работу, но несмотря на это существенно повышает безопасность. Использование Firewall и виртуальной машины практически гарантирует исключение проникновения и исполнения вредоносного кода на вашей основной, рабочей машине.

REFERENCES

- Валентин Холмогоров. PRO Вирусы. / Холмогоров Валентин — М.:Страта, 2015 — 180 стр.