ВИРУСЫ УДАЛЕННОГО ДОСТУПА

А.И.Валиева

Студент 3 курса

Направление «Прикладная информатика»

Факультета Физики и математики

Россия, Бирск, БФ УУНиТ

На сегодняшний день человечество не может представитьсвою жизнь без компьютеров. Люди пользуются ими на работе и дома. Компьютеры облегчили жизнь, теперь существует возможность платить за счета, общаться с друзьями, учиться, не

выходя при этом из дома. Пользуясь всем этим, владельцы компьютеров должны понимать, что открывается лазейка для компьютерных вирусов. Это самая большая угроза для вашей техники.

Компью́терный ви́рус — вид вредоносных программ, способных внедряться в код других программ, системные области памяти, загрузочные секторы и распространять свои копии по разнообразным каналам связи.

Почти все компьютерные вирусы создаются злоумышленниками, имеющими цель заполучить конфиденциальные данные пользователя или использовать его компьютер в личных целях.

Существуют много разных видов компьютерных вирусов и каждые из них могут иметь разную цель: для кражи данных, использования нашего компьютера в атаках, рассылки спама и рекламы и даже для слежки за человеком, тем самым нарушая закон о неприкосновенности частной жизни человека.

Троян удаленного доступа – это разновидность вредоносного программного обеспечения (ПО), которое позволяет злоумышленнику удаленно получить контроль над персональным компьютером человека.

В понятии «Троянский» заключается то, что этот вирус передается скрытно и

незаметно для пользователя.

Например, скачивая какую-то утилиту, игру или программу мы с легкостью становимся уязвимыми для заражения «скрытым» вирусом.

При заражении нашего личного устройства этим вирусом отправитель сможет заполучить абсолютный доступ. Интересы отправителя могут колебаться от изучения нашей файловой системы, наблюдение за нашими действиями, сбора частных данных, чтобы в будущем требовать выкуп. Так же большая угроза представляется, когда заражен ваш рабочий компьютер, ведь материалы рабочего компьютера могут обладать большей важностью тем, что там могут храниться в себе множество сведений о ваших клиентах.

После установки RAT(RemoteAdministrationTool - средства удалённого администрирования или управления) ваш компьютер может стать концентратором, откуда атаки будут запущены на другие компьютеры в локальной сети, что позволит обойти любую защиту периметра.

Разработчики и пользователи вредоносного ПО RAT могут взять под контроль объекты промышленной и гражданской инфраструктуры. Таким образом, RAT не только представляют угрозу для корпоративной безопасности и безопасности государств. Особенно такие технологии могут использоваться в качестве «оружия» при «гибридных войнах». Хакеры по всему миру могут применить RAT для слежки за компаниями и

кражи их данных и средств. Между тем проблема RAT теперь стала вопросом национальной безопасности для многих стран, в том числе России.

В частности рассмотрим наиболее известные компьютерные вирусы, заимствованные из источников [1, 2].

Несколько известных RAT

BackOrifice

BackOrifice – это американский RAT, который существует с 1998 года. Это своего предок RAT. Первоначальная схема эксплуатировала уязвимость в Windows 98. Более поздние версии, которые работали в более новых операционных системах Windows, назывались BackOrifice 2000 и DeepBackOrifice. Эта RAT способна скрываться в ОС(операционной системе), что делает ее особенно недоступной для обнаружения. Однако на сегодняшний день большинство антивирусов используют в качестве сигнатур исполняемые файлы BackOrifice. Отличительной особенностью этого ПО является то, что оно имеет упрощенную в использовании консоль, которую злоумышленник может использовать для навигации и просмотра зараженной системы. После установки эта серверная программа связывается с консолью клиента по стандартным сетевым протоколам. Например, известно, что используется номер порта 21337.

DarkComet

DarkComet был создан в 2008 году французским хакером Жан-ПьеромЛесюером, но только в 2012 году, когда было обнаружено, что африканское хакерское подразделение использовало систему для нападения на правительство США, это привлекло внимание сообщества кибербезопасности. DarkComet имеет простой в использовании интерфейс, который позволяет пользователям, практически не обладающим техническими навыками, проводить хакерские атаки. Это позволяет следить за регистрацией клавиш, захватом экрана и сбором паролей. Хакер control также может включать или выключать компьютер на расстоянии.Также есть возможностьпользоваться сетевыми возможностями зараженного компьютера, чтобы использовать его в качестве прокси-сервера и скрывать его личность во время атак на другие устройства.

Mirage

Mirage – известная RAT, используемая спонсируемой государством китайской хакерской группой. После очень активной шпионской кампании с 2009 по 2015 год группа исчезла из поля зрения. Mirage был основным инструментом группы с 2012 года. Обнаружение варианта Mirage, названного MirageFox в 2018 году, является намеком на то, что кампания может вернуться на просторы. MirageFox был обнаружен в марте 2018 года, когда был использован для слежки за правительственными подрядчиками Великобритании. Что касается оригинальной Mirage RAT, она была создана для атак на нефтяную компанию на Филиппинах, тайваньских военных, канадскую энергетическую компанию и другие цели. Этот RAT поставляется встроенным в файлы типа PDF. Открытие зараженного файла приводит к осуществлению скриптов, которые устанавливают вирус. После установки его первоначальнаязадача – отчитаться перед системой управления и контроля с проверкой возможностей зараженной системы. Эта информация включает в себя скорость процессора, объем памяти и использование, имя системы и имя пользователя.

Защита от RAT – средства обнаружения вторжений IDS

Многие антивирусные программные обеспечения иногда не несут пользы при обнаружении и удалении RAT.Это связано отчасти с их природой.Они прячутся как нечто абсолютно безобидное.По данной причине они часто лучше всего находятся системами, которые анализируют компьютеры на предмет странного и непривычного для устройства поведения.Такие системы называются системами обнаружения вторжений IDS.В большинстве случаев, они успешнее идентифицируют вирусы удаленного доступа, чем другие типы средств защиты от вредоносных ПО.

В результате исследования был проведен обзор вредоносного ПО (вирусов) с возможностью дистанционного управления чужим компьютером. Часто признаками заражения вредоносным ПО является снижение производительности системы и неадекватное поведениенашего персонального компьютера. Для защиты компьютерной техники необходимо использовать антивирусы и пользоваться стандартными общепринятыми правилами работы с данными в сети.

Литература

1) Трояны удаленного доступа [Электронный ресурс] URL: https://itsecforu.ru/2019/02/11/%D1%82%D1%80%D0%BE%D1%8F%D0%BD%D1%8B-%D1

%83%D0%B4%D0%B0%D0%BB%D0%B5%D0%BD%D0%BD%D0%BE%D0%B3%D0%BE-%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%B0-rat-%D1%87%D1%82%D0%BE-%D0%BE%D0%BD%D0%B8-%D0%B8-%D0%BA/ (Дата обращения 13.02.2023)

2) Основные виды вирусных программ[Электронный ресурс] URL:https://zillya.ua/index.php?q=ru/osnovnye-vidy-virusnykh-programm (Дата обращения 14.02.2023)

3) Определение компьютерного вируса [Электронный ресурс] URL:https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D1%8B%D0%B9_%D0%B2%D0%B8%D1%80%D1%83%D1%81
(Дата обращения 12.02.2023)