Hacker Highschool

SECURITY AWARENESS FOR TEENS



УРОК 6
ВРЕДОНОСНЫЕ ПРОГРАММЫ

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM

ВНИМАНИЕ

Проект Hacker Highschool является средством обучения и, как в любом обучающем средстве, существует опасность. Некоторые уроки, если ими злоупотреблять, могут привести к физической травме. Также дополнительные опасности могут быть там, где ещё недостаточно исследований о возможных последствиях излучений от специфической техники. Студенты, использующие эти уроки, находятся под контролем преподавателя и, в тоже время, должны быть мотивированы на изучение материалов и непрерывную практику. ISECOM не несёт ответственности за применение информации, полученной из данных материалов и за дальнейшие последствия.

Все представленные здесь материалы являются открытыми и общедоступными в соответствии с положениями и условиями организации ISECOM:

Все материалы проекта Hacker Highschool предназначены для некоммерческого использования в работе с учениками средних государственных или частных школ, техникумов, студентами высших учебных заведений, слушателями младших курсов Hacker Highschool и учащимися на дому. Эти материалы в любой форме не могут быть использованы для продажи. Обучение по этим материалом в обучающей организации, техникумах, университетах, профессионально-технических заведениях, летних или компьютерных лагерях и других организациях, в которых взимается плата за обучение, категорически запрещено без приобретения лицензии. Для более подробного ознакомления с условиями использования либо приобретения лицензии для коммерческого использования материалов, посетите раздел сайта предназначенный для Лицензирования http://www.hackerhighschool.org/licensing.html.

Проект HHS является результатом труда открытого сообщества и, если Вы находите наши труды ценными и полезными, мы просим Вас поддержать нас путём приобретения лицензии, пожертвований либо спонсорства.

СОДЕРЖАНИЕ

СОТРУДНИКИ ЖУРНАЛА

Pete Herzog, ISECOM
Glenn Norman, ISECOM
Marta Barceló, ISECOM
Kim Truett, ISECOM
Marco Ivaldi, ISECOM
Greg Playle, ISECOM
Bob Monroe, ISECOM
Simon Biles
Rachel Mahncke
Stephan Chenette
Fred Cohen
Monique Castillo

ПЕРЕВОДЧИКИ

Vadym Chakrian, Kharkiv National University of Radio Electronics
Olena Boiko, Kharkiv National University of Radio Electronics

ISECOM

ВВЕДЕНИЕ

Удивительно, насколько просто **вредоносные программы** (далее по тексту «вредоносное ПО») заражают системы. Фред Коэн написал диссертацию о компьютерных вирусах в 1984 году. Она была опубликована в 1985 году. Сперва диссертационную работу сочли низкосортной и смешной, и так считали до тех пор, пока Коэн не пояснил свою идею. Данные события происходили в то же время, когда появился червь Морриса. Как только представители академического сообщества увидели потенциал вирусных атак, они не на шутку испугались.

Кое-кто боялся, что диссертация Коэна может натолкнуть плохих парней на плохие мысли. Поэтому они отложили публикацию работы до 1985 года, однако идея уже была реализована и продемонстрирована и до публикации работы Коэна.

Развитие данных продуктов привело к созданию нового вида оружия, такого, как, например, **Stuxnet**. Самый маленький самораспространяющийся вирус содержал всего 90 строк кода.

Вредоносное ПО может научить специалистов по информационной безопасности социальной инженерии, эксплуатации программного обеспечения, скрытности и технологическим новациям, которые демонстрируют высокий уровень навыков некоторых программистов. Новые формы вредоносного ПО могут быть довольно сложными, и для его создания потребуется целая команда хорошо спонсируемых программистов. Есть, конечно, и такие вредоносные программы, которые написаны в чьей-то комнате и созданы, чтобы обойти рубежи безопасности системы и сеять хаос.

Вредоносное ПО изначально не приносило денег или другой материальной выгоды (кроме вирусов-вымогателей, конечно) человеку, который его создал. Однако эта ситуация со временем изменилась, так как создатели вирусов научились извлекать выгоду из хищения данных, используя информацию о кредитных карточках, чтобы получить доступ к банковским системам с помощью вируса Zeus. С тех самых пор подобных случаев становится всё больше, и данная категория вирусописателей процветает и по сей день.

Большинство типов вредоносного ПО пытаются получить выгоду путём мошенничества, спама, ботнетов и шпионажа. Подобное положение дел породило антивирусную индустрию, в которой сегодня крутятся миллиарды долларов. Как думаете, есть ли тут какая-то связь?

Анализируя вирус, Вы можете увидеть изнутри, как работает поистине изумительная программа. Полиморфизм, прелестная идея! Почему же у нас нет полиморфных систем обнаружения вторжений? Трудно понять, почему вирусописатели используют эту чудесную технику, а гиганты индустрии программного обеспечения нет. Так же, как и настоящий вирус, мы можем изучить, как мыслят пользователи и как подобное программное обеспечение использует человеческое поведение, чтобы выжить (и процветать).

Большинство вредоносов (англ. malware, **mal**icious soft**ware** — злонамеренное программное обеспечение) — это компьютерная программа или часть программы, которая обладает деструктивным или нежелательным воздействием на Ваш компьютер. Обычно при упоминании вредоносного ПО люди сразу представляют себе **вирус**, однако это понятие охватывает не только вирусы. Наши забавные Интернет-друзья создали **червей** и **троянских коней**, **руткиты**, **логические бомбы**, **шпионские программы** и **ботнеты**. Вредоносным ПО можно назвать что угодно из этого списка и любые комбинации этих вредоносов. Сегодня тяжело назвать вредоносное программное обеспечение просто вирусом, червем или

даже червем-троянцем. Именно поэтому для описания этого понятия лучше всего подходит термин «вредоносное программное обеспечение» (вредонос).

Вы уже готовы погрузиться в мир вредоносного ПО?

Организация AV-TEST зарегистрировала более 180 миллионов вредоносных программ, начиная с 1984 года. Каждый день в этот список добавляются около 20 тысяч новых экземпляров. Вы можете проверить сами: http://www.av-test.org/en/statistics/malware/.

Проблема в том, что мы не знаем, как они распределяют вредоносные программы по категориям. К примеру, полиморфный вирус может быть похожим на множество других вирусов, или на самого себя, или может и вовсе не детектироваться. И системы обнаружения вторжений увидят совсем не то же самое, что антивирусные программы. Так что относитесь к подобным цифрам с долей скептицизма.

ВИРУСЫ

Это именно то слово, о котором думает большинство людей при упоминании о вредоносном ПО. Компьютерные **вирусы** пришли к нам из компьютерных наук, из области искусственного интеллекта — там они более известны как клеточные автоматы — которые постепенно стали более «жизненными», у них появилась способность распространяться (создавать себе подобных), заражать больше машин, закрепляться в системе и даже охотиться и уничтожать друг друга. По своему поведению они очень напоминали естественные вирусы, и поэтому к ним прикрепилось такое название.

Вирусы (англ. «viruses», «virii») — это самовоспроизводящиеся части программного обеспечения, которые, подобно биологическим вирусам, прикрепляют себя к другим программам или (в случае с макровирусами) к другим файлам. Вирус запускается только тогда, когда запускается программа или файл, которые он заразил. Вот что отличает вирусы от червей. Если зараженные программы или файлы не запускаются, тогда и вирус будет дремать.

Разные вирусы используют разные механизмы запуска, к примеру, определённые дату и время или нажатие определённой комбинации клавиш. Подобные механизмы используются для определённых случаев, таких как напоминание об активизации, преступлениях, военных действиях или когда девушка вирусописателя возбуждает против него судебный процесс.

Некоторые вредоносные программы состоят из отдельных программ, которые могут быть обновлениями ПО или чьими-то картинками с пляжной прогулки. Файлы Adobe PDF были довольно частой точкой для первоначального заражения вирусами, так же как и Java. Существует множество отчётов о пиратском ПО, которое разработано так, что выглядит вполне легально, однако на самом деле содержит вредоноса. Вот почему следует проверять **контрольную сумму** перед загрузкой программы или файла. Да, **MD5 хэш** тоже можно подделать, однако мы хотим, чтобы Вы были максимально осторожными, когда загружаете лицензионную копию чего-либо себе на компьютер.

Хорошо спроектированный вирус будет избегать детектирования, исполнять свою задачу и распространяться на другие машины, а жертва даже и не догадается о том, что происходит, пока не станет слишком поздно. Или вовсе никогда об этом не узнает.

Авторитетный доктор наук Фред Коэн перечислил некоторые дополнительные способы, которыми вредоносные программы могут испортить Вашу систему и данные:

- выставить случайные настройки защиты
- файлы, доступные для чтения, становятся недоступными для чтения
- файлы, недоступные для чтения, становятся доступными для чтения
- файлы, доступные для записи, становятся недоступными для записи
- файлы, недоступные для записи, становятся доступными для записи
- запускаемые программы не запускаются
- незапускаемые программы запускаются
- привилегии setUID (уровень доверия) добавляются для непроверенного ПО
- при внедрении в производственную линию конкурентов вредоносные программы могут занижать качество продукции, если зараженная система контролирует процесс производства (ой!)

Сейчас большинство вредоносных программ используется в качестве метода доставки полезной нагрузки. Вирус может использоваться для обнаружения чувствительных данных в сети, открывать и оставлять открытыми сетевые соединения для будущей атаки, осуществлять DdoS-атаки (атаки типа отказ в обслуживании), перехватывать финансовую информацию, выводить из строя производственные и инфраструктурные службы. Продвинутые вредоносные программы обычно обладают защитными механизмами, содержат в себе несколько эксплойтов и запрограммированы на столь долгое выживание и распространение, насколько это возможно.

ПОЛИМОРФНЫЕ ВИРУСЫ

После того, как стало понятно, что такое вирусы (после 1988 года), их было довольно легко обнаружить. Каждый из них имел определённую сигнатуру, по которой можно было однозначно их определить, с целью предотвращения их размножения. В других случаях они имели простую структуру, в которой можно было легко определить, к примеру, полезную нагрузку. Однако затем появились **полиморфные** вирусы, где «поли» означает «множество», а «морфность» означает «форма». Это новое поколение вирусов, которые изменяют самих себя при каждом новом воспроизведении, реорганизуют свой код, изменяют тип и ключ шифрования и порождают совершенно новые вирусы. Данное свойство создало крайне большие проблемы для обнаружения вирусов, так как теперь уже невозможно было создать хорошую сигнатуру для определения вируса.

Один из самых простых способов заставить вирус изменить самого себя — шифрование. Всё, что нужно сделать вирусописателю, так это создать генератор случайных ключей шифрования, чтобы вирус шифровался каждый раз на новом ключе и тем самым изменял сам себя, избегая детектирования при каждом новом копировании. **Антивирусным** (англ. «antivirus», «AV») компаниям стало сложно выявлять схожие строки кода для создания сигнатур.

Тогда антивирусные компании решили взглянуть на те части полиморфного вируса, которые не менялись бы в процессе шифрования/расшифрования. Как Вы можете догадаться, вирусописатели пробовали изменить функции расшифрования и сделать их такими же случайными, как и остальная часть вредоносного кода. Программисты-мошенники добавляли другие даты, случайное время, различные алгоритмы и операции, а также применяли множество других

техник, которые позволили бы сделать вирус полностью полиморфным и не детектируемым.

Создатели вирусов обратились к другому методу сокрытия вредоносных программ и начали разбивать код вируса на несколько частей. Первой частью вируса является, к примеру, безвредный PDF-файл, однако внутри него вшит скрипт, который осуществляет загрузку второй части вируса на компьютер жертвы. Вторая часть вируса зашифрована, таким образом антивирусные программы не могут обнаружить его.

Создатели вирусов ищут способы сделать вирусы похожими на что угодно, кроме вирусов. Так как антивирусы ищут файлы, события, поведение или подозрительную активность, которые могут быть вирусом, разработчики полиморфных вирусов решили имитировать функции операционной системы, аппаратного обеспечения и пользователей.

В некоторых случаях вирусы заменяют настоящие системные файлы. Прелесть: каждый раз, когда Вы открываете Блокнот (англ. «Notepad»), вирус размножается.

МАКРОВИРУСЫ

Макровирусы используют встроенные возможности ряда программ исполнять программный код. Такие программы, как Word и Excel, имеют ограниченную, однако достаточно мощную версию языка программирования Visual Basic (сокращенно «VB»). Использование макросов, написанных на VB, позволяет автоматизировать множество задач и настройку опций. Такие макроязыки могут быть использованы для прикрепления вредоносного кода, который автоматически скопирует сам себя в другие документы и, таким образом, самораспространится.

Так как Word и Excel являются частью пакета программ (Microsoft Office), макровирус может воспользоваться их системными привилегиями и с лёгкостью распространиться по всей корпоративной сети. Офисные программы могут использовать специальные (недокументированные) скрипты операционной системы для повышения производительности, что также даёт макровирусам доступ к защищённым областям операционной системы и сети.

В большинстве клиентских программ для электронной почты Вы можете совершить предпросмотр вложения, не открывая самого письма. Именно в этот момент макровирус производит атаку, поскольку минипрограмма открывает вложенный файл. Предпросмотр активирует вложение, даже если файл был назван «милыйщенок.jpg». Название и расширение файлов могут быть подделаны. Можете сами в этом убедиться, ознакомившись с **Уроком 9: Взлом электронной почты**.

Макровирусы можно обнаружить там, где есть скрипты, код, формы и подпрограммы, исполняемые на стороне клиента. Довольно часто они встречаются в HTML5, Java, Javascript и других дополнениях, которые являются частью браузеров. Вы можете узнать больше об этом в **Уроке 10: Безопасность веб-приложений**.

УПРАЖНЕНИЯ

Исследуйте следующие вопросы:

6.1 Какой был первый вирус? Не доверяйте первому же ответу, который найдёте. Проверьте несколько источников. Можете засчитать себе пять дополнительных очков за каждое доказательство неправильности версий Ваших одноклассников.

6.2 Теперь: какой первый вирус был *выпущен в свободное плавание*? Как он распространялся?

6.3 Вирус **Klez** хорошо известен тем, что совершал подмены (**spoofing**). Что такое подмена и как Klez использовал её? Представьте, что Ваш компьютер заражен вирусом Klez. Как бы Вы удаляли его? Как Вы можете его обнаружить?

6.4 Может ли вирус быть полезным или выполнять полезные действия, помимо вредоносных? Подумайте о реальном предназначении вируса прежде, чем принять решение.

6.5 Каково было предназначение вируса Stuxnet? Исходя из того, что Вы прочли, достиг ли вирус своей цели?

6.6 Представьте, что Вы только что получили письмо со следующей темой: «Предупреждение о вашем e-mail аккаунте» (англ. «Warning about your email account»). В теле письма поясняется, что так как Вы используете почтовый ящик не по назначению, то Вы можете потерять свои Интернет привилегии. Для того, чтобы ознакомиться с деталями, следует просмотреть вложение письма. Однако Вы, насколько Вам известно, не делали ничего необычного с Вашим почтовым ящиком. Вы что-то заподозрили? Должны были бы. Исследуйте данную информацию и определите, какой вирус прикреплён к данному письму. (Подсказка: когда начнёте думать о завтраке — Вы на правильном пути).

ИГРА НАЧАЛАСЬ: ВРЕДОНОСНЫЙ УЧИТЕЛЬ

В классной комнате по технологии стоял запах то ли протухшей рыбы, то ли крысиной шерсти, но, по крайней мере, там был порядок. На каждой парте «отдыхал» монитор компьютера. Флуоресцентные лампы мерцали на свету, пробивавшемся от ряда окон. Один студент за первой партой зевнул, и волна зевания прокатилась до последних рядов. Мистер Три, учитель, с хмурым видом и сгорбившись сидел за своим столом, уставившись в монитор.

Если бы в помещении не было такого дурного запаха, студенты начали бы обедать, жевать жвачку или болтать друг с другом, пока учитель осваивал базовые навыки компьютерной грамотности. Но они вынуждены были зажать носы или дышать через рукава. Им совсем не хотелось разговаривать, есть или жевать в такой обстановке. Взгляд некоторых уже приклеился к часам: до конца урока оставалось пятьдесят две минуты.

Спустя восемь минут Джейс попыталась как можно тише пробраться через дверь в классную комнату. Почувствовав неприятный запах, она громко кашлянула. Мистер Три услышал неожиданный звук и почувствовал изменение давления после открытия двери. Он обернулся и успел увидеть Джейс до того, как она спряталась под партой. «Джейс, ты решила присоединиться к нам сегодня. Какой замечательный сюрприз.»

Джейс бросила взгляд на ребят и увидела глаза, говорящие ей бежать, пока у неё есть возможность, вырваться на свободу. Беги, Джейс, беги. Спасайся!

Она посмотрела на мистера Три и ответила: «Извините за опоздание. Я плохо себя чувствовала.» Это была слабая отговорка, но внимание учителя было поглощено другой проблемой. Джейс сняла рюкзак и направилась к своей парте. Зажав нос, она спросила своего однокурсника, что происходит. Он ответил: «Ты очень скоро узнаешь сама.»

«Джейс, поскольку ты пропустила начало урока, я проясню тебе ситуацию. Кто-то из студентов установил грипп или простуду на эти компьютеры,» — начал учитель. В каждом его слове слышалась нота осуждения. — «И теперь, пока кто-либо из вас не сознается в совершении преступления, вы все будете сидеть здесь и наслаждаться этим чудесным запахом, который я принёс сюда,» — сказал мистер Три. Джейс посмотрела вокруг и увидела источник этого запаха — в центре классной комнаты лежала шуба, из карманов которой выпадали сардины.

«Мисс Джейс, Вы что-нибудь знаете об этом компьютерном заболевании?» — спросил учитель, указывая на монитор. Джейс встала и направилась к мистеру Три так, будто она приближалась к голодному скунсу. Когда Джейс увидела текст на мониторе, она быстро пододвинула клавиатуру ближе к себе, ввела несколько команд и просмотрела, какой ответ выдал компьютер.

«Хмм,» — только и сказала она. В одно мгновение Джейс дотянулась до своего рюкзака, достала чехол для очков, открыла его и достала из него USB-флешку. Её правая рука уже печатала что-то на клавиатуре, в то время как левая вставляла флешку. «Кто-нибудь обновлял программное обеспечение на этих компьютерах?» Продолжительная тишина натолкнула её на мысль, что на лице мистера Три изобразилось непонимание.

«В смысле *обновлял*?» — спросил он.

«Не важно.»

Во-первых, браузер был давно устаревшим, а расширения Soda HTML

прекрасно подвергались уязвимостям нулевого дня. Во-вторых, она увидела ещё один продукт HTML5, который назывался Teepee и которому было уже как минимум два года. Просматривая папки с утилитами на флешке, Джейс нашла и запустила Nmap, чтобы посмотреть, какие порты прослушиваются на компьютере. Nmap выдал длинный список открытых портов. Джейс нахмурила брови.

Wireshark показал крупный объём трафика TCP/IP, входящего и исходящего из пяти портов на компьютере. Чтобы исправить это, она просто отключила сетевое соединение. Пять портов продолжали отправлять пакеты SYN даже без сетевого соединения. Она переключила своё внимание на файлы загрузки операционной системы.

Джейс не знала, что она говорила «хммм» каждый раз, когда что-то проверяла в компьютере, но все остальные в классе заметили это. Они собрались возле неё в «полукруге любопытства». «Хммм,» — сказала Джейс, заметив несколько необычных программ в настройках загрузки системы.

Она просканировала всё в поисках необычного времени доступа к какой-либо папке или файлу. И вновь в результате получился целый список очень подозрительных программ, папок и файлов.

Каждый бит плохих файлов был связан с одним и тем же именем пользователя. Джейс как раз вовремя закрыла рот рукой, затем медленно повернулась направо, опустила руку и тихо сказала: «Мистер Три, похоже, что человек, который загрузил все эти вредоносные программы, — это пользователь с именем Супер Три.» И только когда все засмеялись, она оглянулась и увидела, что весь класс собрался за её спиной.

Упс.

Игра закончилась

ЧЕРВИ

Черви похожи на вирусы тем, что они тоже распространяются, но для перемещения они используют сетевые службы. Они не ждут, что кто-нибудь откроет или получит доступ к определённому файлу, после чего запустится вредоносный код; червь запускается сам, как только он обнаружит уязвимый хост.

Таким образом, червь — это автономная программа, которая после запуска распространяется без необходимости вмешательства человека. Он будет перемещаться от одного хоста к другому, используя незащищённые сети или службы. Черви захватывают серверы и целые сети, поскольку одна из их задач заключается в размножении. В зависимости от того, как был спроектирован червь, у него может и не быть конкретного конечного пункта или цели.

Черви используются для составления карты сетей, для проникновения в скрытые области и для «составления отчёта» по своим находкам в определённых узлах. Этот тип вредоносного ПО может работать автономно или в составе «команды» и под управлением.

Существует несколько типов червей, которые никто не смог ни удалить из систем, которые они заразили, ни определить их назначение или их местонахождение. Черви идеально подходят для рекогносцировки, поскольку они обычно не имеют полезной нагрузки и используют тайные каналы для передачи информации (если они вообще передают информацию). Если червь никогда не будет передавать

информацию, то определить, где он размещён и что он намерен делать, будет просто невозможно.

Хорошая новость про червей: они обычно заражают систему только один раз. Плохая новость: единственное, что мы можем сказать Вам, перед тем, как Вы начнёте поиски этого заражения и удаление червя: «Удачи!»

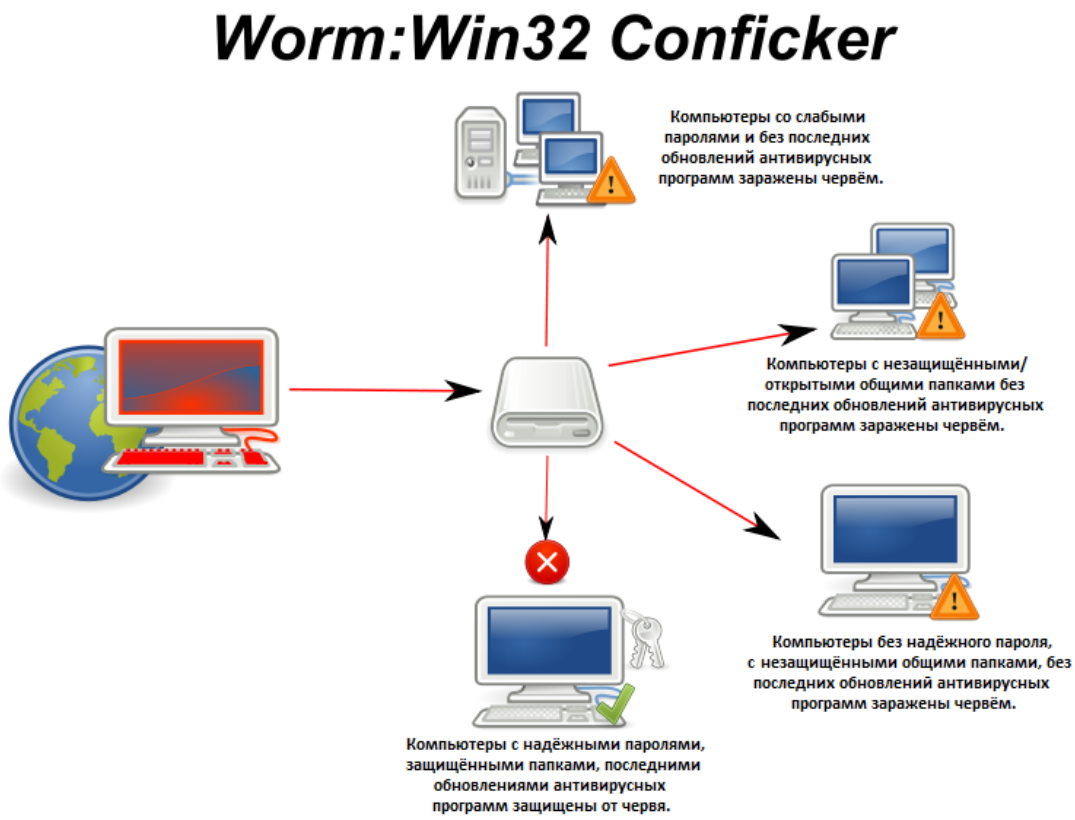

Рисунок 1. Как распространяется червь **Conflicker**. Фотография публикуется в рамках лицензии Creative Commons. http://en.wikipedia.org/wiki/File:Conficker.svg

УПРАЖНЕНИЯ

6.7 Какие операционные системы были уязвимыми к первому червю, который распространялся через Интернет? Найдите исходный код. Да, мы не шутим. Нет, это не нанесёт вред Вашему компьютеру. Вы можете открыть файлы в браузере и посмотреть, как забавлялся автор. Вы можете бранить его или завидовать ему, как хотите.

6.8 Поищите видео, в которых показано, как использовать хакерские утилиты для червей. (Подсказка: в поиске используйте буквально вот эту последнюю фразу.) НЕ ПЕРЕХОДИТЕ ПО НАЙДЕННЫМ ССЫЛКАМ. Помня о том, что черви распространяются через зараженные файлы (в том числе и видео), задумайтесь — стОит ли доверять тем видео? Или даже тем ссылкам?

6.9 Как Вам определить: доверять или не доверять этим видео? Для начала найдите в Интернете статью «Десять уловок, чтобы завоевать доверие любого человека (временно)» («Ten Tricks to Make Anyone Trust You (Temporarily)»). Оказывались ли Вы когда-нибудь под воздействием какой-либо из этих уловок?

ТРОЯНЫ И ШПИОНСКИЕ ПРОГРАММЫ

Вредоносные программы существуют во многом благодаря спаму. Сейчас мы поговорим о **троянах (trojan)**, **шпионских программах (spyware)** и программах, содержащих рекламу **(adware)**. Первый **троянский конь** был создан греками несколько тысячелетий назад. (Вспомните фильм «Троя», если Вы его смотрели.) Смысл заключается в том, что Вы предлагаете что-то, что кажется полезным или неопасным, чтобы «подбросить» какую-то неприятную вещь в компьютер, который до этого казался защищённым. Например: трейлеры игр; электронные письма с изображением обнажённых знаменитостей; программы или утилиты; файлы (например, PDF) или пиратские видео. Часто они встраиваются в так называемые свободно распространяемые игры (**freeware** games). Концепция freeware не заключается в заполнении бесплатного продукта рекламой и спамом, но каким-то образом эти идеи смешались.

Трояны — это вредоносные программы, которые выдают себя за что-то полезное или привлекательное, чтобы Вы запустили их. Существуют как минимум два типа троянов. Первый тип притворяется полезной программой, картинкой, песней, фильмом или является прикреплённым файлом в программе. Второй тип — это поддельная программа, которая заменяет настоящую на Вашей системе. Как только она попадёт в систему, она сможет выполнить какие-то неприятные вещи: установить бэкдор или руткит или — что ещё хуже — превратить Ваш компьютер в зомби. Слышите эту жуткую фоновую музыку?

Одним из признаков того, что на Вашем компьютере установлен троян, является существенное замедление работы и потеря ресурсов. Это касается Вашего компьютера, не Вас. Если Вы у себя замечаете существенное замедление работы и/или потерю ресурсов, то у Вас грипп. Вам нужно сходить к врачу. Отремонтировать Ваш компьютер будет не так легко. Вам придётся использовать все свои силы.

Может оказаться, что некоторые приложения не запускаются или что запускаются программы, которые вовсе не должны были запускаться. Не ожидайте, что Ваша антивирусная программа поможет, ведь она не смогла предотвратить установку этого трояна; почему же сейчас она будет работать?

Нет, теперь проблема ложится на Ваши плечи, и если на Вашем компьютере завёлся один троян, то можете ожидать, что вскоре себя проявят ещё несколько. Поскольку трояны — это всего лишь сосуды, в которых переносится мусор для сброса на Ваш компьютер, Вам будет необходимо выяснить, откуда взялся троян. Вспомните, какие файлы Вы недавно загружали, открывали или просматривали у друга?

В защиту Вашего друга можем сказать, что даже очень крупные организации заражали трояны компьютеры своих сотрудников, клиентов и других организаций. Среди них были Sony, Valve (дважды). Возможно, и Microsoft, но они продолжают называть это «недокументированными возможностями» («undocumented features»).

Мы поговорим об удалении вредоносных программ чуть позже.

РУТКИТЫ И БЭКДОРЫ

Часто случается так, что после взлома компьютера хакер хочет вернуться на место преступления. Для этого есть несколько вариантов, некоторые из которых стали довольно известными — поищите в Интернете «**Back Orifice**».

Руткиты и бэкдоры — это вредоносные программы, которые создают способы сохранения доступа к компьютеру или сети. Они бывают разные: от простых

(программы, которые слушают порты) до очень сложных (программы, которые скрывают процессы в памяти, изменяют лог-файлы и слушают порты). Вирусы Sobig и MyDoom устанавливают бэкдоры как часть своей полезной нагрузки.

Производителей аппаратного и программного обеспечения часто обвиняют в установке бэкдоров в своей продукции. В некоторых случаях этот хакинг финансировался государством, в других — это была инициатива самих компаний. Sony установила шпионское ПО на устройства пользователей, чтобы обеспечить **технические средства защиты авторских прав (Digital Rights Management, DRM)**. Известно, что некоторым китайским компаниям заказывали сборку маршрутизаторов, концентраторов и других устройств с встроенными тайными кодами. После применения таких методов пользователи утратили доверие к брендам и товарам в определённых странах.

Имея дело с руткитами, будьте готовы к потере **главной загрузочной записи (master boot record, MBR)** — программного обеспечения, которое загружает Вашу операционную систему. Руткиты должны загрузиться в память до операционной системы. Они добиваются этого, «спрятав» часть себя в MBR. Это означает, что успешное удаление руткита также повредит Ваш MBR.

Чтобы исправить MBR, Вам понадобится запустить командную строку через восстановление системы. В командной строке введите следующую команду и нажмите Enter:

```
bootrec.exe /FixMbr
```

При успешном завершении процесса Вы увидите сообщение «**Операция завершилась успешно.** Главная загрузочная запись была восстановлена.» ("**The operation completed successfully.** The Master Boot Record has been repaired.").

Хотя вышеуказанная команда исправит MBR, возможно, что ещё будет ошибка, связанная с **загрузочным сектором (boot sector)** системного раздела и **данными конфигурации загрузки (Boot Configuration Data, BCD)**, что означает, что повреждение может быть *физическим*. Такое может произойти, если Вы установите другую операционную систему параллельно с Windows 7, например, Windows XP. Чтобы записать новый загрузочный сектор, введите следующую команду:

```
bootrec.exe /FixBoot
```

УПРАЖНЕНИЯ

6.10 Исследуйте Back Orifice. Что именно он делает? Кто его создал?

6.11 Исследуйте Windows Remote Desktop. Что именно он делает? Сравните его с Back Orifice: чем они отличаются?

6.12 Представьте, что Вы хотите, чтобы на Вашем компьютере можно было запустить две разные версии Windows. Для этого нужно знать одну уловку (как обычно). В каком порядке Вы должны установить версии Windows, чтобы это можно было осуществить?

ЛОГИЧЕСКИЕ БОМБЫ И ВРЕМЕННЫЕ БОМБЫ

Логические бомбы и временные бомбы — это вредоносные программы, которые ничего не делают до тех пор, пока не выполнится определённое условие — например, не встретятся определённые данные или не наступит определённая дата. Они обычно не распространяются. Например: можно написать программу, которая начнёт удалять случайные биты данных на дисках, если администратор не будет входить в систему более трёх недель.

Интересная история произошла с одним программистом в компании General Dynamics в 1992 году. Он создал логическую бомбу, которая должна была активироваться после его ухода из компании и которая должна была удалить важные данные. Он ожидал, что тогда компания заплатит ему немалые деньги, чтобы он вернулся и решил проблему. Однако другой программист нашёл эту логическую бомбу до того, как она запустилась, а программист-злоумышленник был признан виновным в преступлении и был оштрафован на $5000. И это наказание оказалось мягким — штраф, который он должен был бы заплатить, достигал $500000, не говоря уже о тюремном заключении.

В 2009 году уволенный работник крупнейшего ипотечного агентства Fannie May установил логическую бомбу, которая должна была вывести из строя их 4000 серверов. К счастью, вредоносная программа была обнаружена до активации. К счастью для компании, к несчастью для бывшего сотрудника.

Логическая или временная бомба относится к атакам изнутри, которые проводят недовольные сотрудники, подрядчики или уволенные работники, у которых был или есть доступ к сети. Такие угрозы лучше предотвращать, чем потом устранять. Организуйте разграничение обязанностей, так что ни один сотрудник не будет иметь слишком много полномочий при работе в системе. Убедитесь в том, что каждый сотрудник каждый год берёт отпуск, так что злодеи не смогут продолжать заметать свои следы.

Наилучший вариант: если Ваша компания увольняет кого-то, немедленно ограничьте ему доступ к сети. Не допускайте, чтобы сотрудник доделывал какую-то работу или проверял почту. Пусть он покинет здание офиса сразу после того, как Вы заберёте его ключи (коды). Сохраните его сетевую учётную запись в специальной папке, но удалите все привилегии для доступа пользователя, особенно удалённого доступа. Это должно хоть как-то помочь (если только этот работник не знает пароли других сотрудников).

УПРАЖНЕНИЯ

6.13 Какое полезное (и законное) применение может быть у временных и логических бомб?

6.14 Как Вы можете обнаружить такие программы на своей системе?

ВРЕДОНОСНЫЕ ПРОГРАММЫ В НАСТОЯЩЕЕ ВРЕМЯ

Вредоносное ПО предоставляет хакеру доступ к файлам или данным в Вашей сети, на Вашем компьютере, планшете или смартфоне. Да, на Вашем мобильном телефоне тоже могут быть установлены вредоносные программы. **Ни одна компьютерная система не защищена полностью от вредоносных программ — включая все персональные гаджеты.**

Ваш мобильный телефон или смартфон по сути является маленьким компьютером. Если Вы ищете что-то в сети, заходите на страничку в Facebook или открываете прикреплённые к электронному письму файлы, то Ваш телефон уязвим к вредоносным программам. Вредоносное ПО может быть даже предустановлено на устройстве. Проблемы, которые могут возникнуть, такие же, как и с обычным компьютером; например, есть риск взлома паролей. Но, скорее всего, вредоносное ПО будет ждать, что Вы будете проводить какие-то финансовые операции, и либо очистит Ваш банковский счёт, либо украдёт информацию о Вашем аккаунте и отправит её хакеру.

Интернет ТВ тоже не исключение. Теперь Вы можете одновременно смотреть какую-то передачу по телевидению и искать что-то в Интернете. Вы можете соединить между собой разные вещи и создать «умный» дом. Опять же, могут возникнуть такие же проблемы, как и на Вашем компьютере. Хакеры взламывают телевизоры с доступом в Интернет, бортовые компьютеры в автомобилях и даже холодильники. На бортовом компьютере можно взломать практически всё. Имейте в виду, что злоумышленники могут проникнуть в Ваш дом — личное пространство, где Вы чувствуете себя в безопасности — через Ваши устройства, подключённые к Интернету.

Вам может показаться, что на Вашем компьютере или смартфоне нет ничего ценного, но Ваша личность может быть использована. То есть хакер может собрать информацию о Вас на Вашем компьютере или телефоне, а также общедоступную информацию о Вас (например, фотографии в Facebook) — этого может оказаться достаточно, чтобы составить подробную характеристику о человеке. Хакер может попробовать открыть кредитные карточки или взять кредит в банке на Ваше имя. Это называется **кража личности (identity theft)**. Кредиторы будут требовать деньги именно с Вас за вещи, которые купил *хакер*. На то, чтобы доказать, что это не Вы тратили деньги, и чтобы восстановить свою репутацию, может понадобиться несколько лет. Это может помешать Вам получить кредит на покупку той «быстрой и яростной» машины, о которой Вы мечтаете.

Мы подключены к цифровому миру почти 24 часа в день, и мы хотим, чтобы наши устройства были подключены к Интернету, даже когда мы ими не пользуемся. Создателям вредоносных программ это только нА руку. Наши телефоны синхронизированы с планшетами, которые синхронизированы с компьютерами, которые синхронизированы с учётными записями в «облаке». Вся информация у нас буквально на кончиках пальцев, и мы хотим, чтобы доступ к нашей музыке, фильмам и личным данным был везде. Создателям вредоносных программ это тоже только нА руку.

В настоящее время большое количество вредоносных программ нацелено именно на мобильные устройства. Эти устройства имеют минимальное количество средств защиты, но в то же время имеют такой же доступ к Вашим данным, как и компьютер. Скорее всего, на Вашем компьютере установлены брандмауэр, антивирусные программы и программы для защиты от шпионского ПО. И, скорее всего, на Вашем мобильном устройстве не установлено ничего из вышеперечисленного. Так быть не должно.

Создатели вредоносного ПО могут менять свою тактику от требования выкупа и атак типа «отказ в обслуживании» до полного уничтожения сетевых данных организации. Sony подверглась атаке в октябре 2014 года. В этой атаке против Sony использовалось сложное вредоносное ПО, целью которого было нарушить проведение ежедневных операций в системе компании и привести к тому, чтобы важные данные стали бесполезными.

ПИЩА ДЛЯ УМА: ДВАДЦАТЬ ОТТЕНКОВ ВРЕДОНОСНОГО ПО

По данным Лаборатории Касперского, в 2013 году рейтинг 20 вредоносных программ выглядел так:

1.	Вредоносные URL	93.01%
2.	Trojan.Script.Generic	3.37%
3.	AdWare.Win32.MegaSearch.am	0.91%
4.	Trojan.Script.Iframer	0.88%
5.	Exploit.Script.Blocker	0.49%
6.	Trojan.Win32.Generic	0.28%
7.	Trojan-Downloader.Script.Generic	0.22%
8.	Trojan-Downloader.Win32.Generic	0.10%
9.	Hoax.SWF.FakeAntivirus.i	0.09%
10.	Exploit.Java.Generic	0.08%
11.	Exploit.Script.Blocker.u	0.08%
12.	Exploit.Script.Generic	0.07%
13.	Trojan.JS.Iframe.aeq	0.06%
14.	Packed.Multi.MultiPacked.gen	0.05%
15.	AdWare.Win32.Agent.aece	0.04%
16.	WebToolbar.Win32.MyWebSearch.rh	0.04%
17.	AdWare.Win32.Agent.aeph	0.03%
18.	Hoax.HTML.FraudLoad.i	0.02%
19.	AdWare.Win32.Ibryte.heur	0.02%
20.	Trojan-Downloader.HTML.Iframe.ahs	0.02%

УПРАЖНЕНИЯ

6.15 Ознакомьтесь с последними угрозами, поступающими от вредоносных программ. То есть какие новые угрозы, связанные с вредоносным ПО, появились сегодня? Зайдите на веб-сайт какой-нибудь компании по разработке антивирусных программ и найдите их монитор активности угроз. Поищите в Интернете информацию на тему «исследование угроз и реагирование на угрозы» (“threat research and response”).

6.16 Есть ли угрозы, которым подвержены сайты социальных сетей? Просмотрите веб-сайты разных антивирусных программ. Совпадают ли первые места их рейтингов вредоносного ПО? Как часто меняются угрозы, поступающие от вредоносных программ (сколько новых угроз появляется каждый день)? Как часто Вам следует обновлять антивирусные программы?

6.17 Какие проблемы могут возникнуть, когда Вы приносите своё собственное устройство (bring your own device, BYOD), например, ноутбук или смартфон, и подключаете его к сети в доме своего друга или на работе? А как насчёт кафе или ресторанов?

У хакеров есть разные мотивы, но у создателей вредоносных программ целью обычно является финансовая выгода: получить деньги «жертвы». Им уже не надо

вламываться в Ваш дом. Они могут опустошить Ваш банковский счёт или потратить большую сумму денег от Вашего имени. Другой способ заработка на вредоносном ПО — это использование чужих компьютеров для распространения спама или электронных писем для фишинга. Хакеры могут заработать много денег таким способом. До тех пор, пока Ваш Интернет-провайдер Вас не заблокирует.

Кому-то покажется смешным, но иногда взломщики открыто предлагают вредоносные программы в качестве услуги. В Интернете довольно просто найти сеть ботов, которая сдаётся в аренду, или нанять взломщика для создания своей вредоносной программы. Можно ли доверять авторам вредоносного ПО? Могут ли они оставить бэкдор на *Вашем* компьютере?

ВРЕДОНОСНЫЕ ПРОГРАММЫ НА МОБИЛЬНЫХ УСТРОЙСТВАХ

Раньше хакеры фокусировались на сетях, но сейчас они легко могут обойти сетевую защиту, нацеливаясь на мобильные устройства. В следующих упражнениях мы рассмотрим вредоносные программы, нацеленные на планшеты и телефоны с ОС Android. Поскольку почти все эти устройства тем или иным образом подключены к Интернету, то велика вероятность того, что в какой-то момент через них осуществится подключение к сети компании. Конечно, многие сети предлагают удалённый доступ только для изолированных сегментов этих сетей. Но это не относится к веб-сервисам, что стало слабым местом в безопасности многих компаний.

Android запускается на виртуальной машине (virtual machine, VM), спроектированной для небольших устройств и для быстрой работы. Эта виртуальная машина называется «Dalvik»; это виртуальная машина Java, которая требует намного меньше ресурсов. Операционная система написана на C++, так же как и все библиотеки в комплекте средств разработки Android (Android Software Development Kit, Android SDK). Это означает, что за всем этим графическим интерфейсом кроется ядро Linux. Это также означает, что Android может запускать Java-приложения в браузере и как автономные программы.

Сторонние программы могут запускать нативные API (native APIs) для доступа к встроенным функциям Android (например, менеджер ресурсов Resource Manager, менеджер телефонии Telephony Manager и другие основные компоненты). Это основная уязвимость, поскольку у игр нет особых причин получать доступ к местам Вашего пребывания, к Вашим фотографиям, текстовым сообщениям или другим личным данным. Сторонние приложения часто написаны на Java, в то время как системные приложения написаны на C++ (в соответствии с используемым процессором).

УПРАЖНЕНИЯ

6.18 Исследуйте приложения на своём устройстве Android (APKs). Зайдите на веб-страницу http://developer.sonymobile.com/knowledge-base/tools/ и найдите там APKAnalyser. Эта бесплатная утилита покажет, как работают эти приложения и какие вызываются API. Она также может представить работу этих приложений в виде красивого графика.

6.19 Какими способами мы можем определить владельца того или иного устройства?

6.20 Зайдите на веб-страницу http://www.xray.io/#vulnerabilities и просмотрите известные уязвимости для устройств с Android, работающих на процессорах Arm. Если бы Вы писали вредоносный код, какие из перечисленных уязвимостей Вы использовали бы в первую очередь? Помните, что они перечислены в алфавитном порядке, а не по популярности. Большинство телефонов работает на процессорах Arm.

ПО ЯБЛОКУ В ДЕНЬ

Теперь пришло время проверить продукцию Apple. Apple всегда позиционировал себя на рынке как защищённый от вредоносного ПО из-за закрытой операционной системы и расширенных функциональных возможностей средств защиты. По правде говоря, безопасность в iOS для всех мобильных устройств Apple зависит от пользователей, которые приобретают программы на официальном Apple Store. Для устройств, которые прошли джейлбрейк, этот метод защиты можно обойти, что означает, что Apple Store нельзя назвать эффективным способом защиты этих устройств. Если компания рассчитывает только на защиту, предлагаемую Apple Store через официальные каналы, то это вообще нельзя назвать планом обеспечения защиты.

Пользователям нравится делиться фотографиями, приложениями, сообщениями, ссылками и другими видами данных. Общие данные становятся точкой входа для вредоносных заражений, так же, как и в любой операционной системе. Частично причиной того, что вредоносных программ для iOS не так много, является то, что это относительно новая популярная платформа. С увеличением популярности iPhone и iPad они чаще становятся целью вредоносных хакеров. Сейчас продукция Apple играет большую роль в мобильном сообществе, поэтому она привлекает намного больше внимания со стороны разработчиков вредоносного ПО.

Одна из первых вредоносных программ для iPhone называется **Wirelurker**. Это приложение распространяется через особую систему, которая позволяет компании устанавливать клиентские приложения без обязательного одобрения Apple Store. К счастью, эта вредоносная программа только загружает комикс (если только телефон не прошёл джейлбрейк). Атакованные телефоны отправляют информацию о платежах на C&C-серверы (о них читайте далее). Другие примеры программ, которые в прошлом атаковали эти телефоны, Apple не рассматривает, называя их «невозможными». Но основная идея этих примеров заключается в том, что такие атаки возможны.

Всё, что подключено к Интернету, восприимчиво ко взлому через вредоносные ссылки, кликджекинг (click-jacking), переадресацию, эксплойты Java и тысячу других уязвимостей. Продукция Apple — не исключение.

УПРАЖНЕНИЯ

6.21 Wirelurker скомпрометировал около 800 миллионов устройств Apple, заражая iPhone и iPad через USB-соединение с компьютером. Как Вы думаете: почему такая мощная программа использует простую полезную нагрузку — установку приложения-комикса, в то время как может устанавливать более опасные программы?

6.22 Посмотрите информацию об эксплойте CVE-2014-4377: какие операционные системы и/или устройства могут оказаться уязвимыми? Как работал бы этот эксплойт, если бы у пользователя не было доступа к Интернету? Safari открывает PDF-файлы даже без доступа к Интернету. Поскольку Safari определяет PDF-файлы как изображения, без ведома пользователей может быть загружено множество файлов PDF, что может привести к эксплуатируемому переполнению буфера.

6.23 На веб-странице http://www.exploit-db.com/platform/?p=ios представлен список известных уязвимостей в iOS, которым подвержены устройства iPhone и iPad: от доступа к Wi-Fi до управления камерой. Первые записи в базе данных уязвимостей iOS относятся к 2010 году. В каком году было задокументировано наибольшее количество эксплойтов? Как Вы думаете — какова была причина?

БОТНЕТЫ

Ботнет (botnet) – это сеть компьютеров (обычно от нескольких сотен до миллионов), на которые были совершены атаки и на которые без ведома владельцев были установлены **руткиты (rootkit)** и **бэкдоры (backdoor)**. Для вредоносных программ это неосведомлённые хосты, или **зомби (zombies)**. Хакер (**bot master** или **bot herder**) может удалённо отправлять этим машинам команды делать всё, что он хочет: от рассылки спама до проведения DdoS-атак и кражи финансовой информации.

Если на Вашем компьютере установлен бот, он [компьютер] может быть использован при проведении атаки. Заражённый компьютер может атаковать полицейские серверы. С юридической точки зрения Вы ответственны за поведение своего компьютера, так же как и за поведение своего кота или собаки. Что если Ваш компьютер замешан в атаке на важнейшие объекты инфраструктуры в Вашей стране, например, на объекты электроснабжения и водоснабжения?

Такие виды атак называются **кибервойнами (cyberwar)**, хотя это опасное слово, поскольку то, чем занимается полиция, очень отличается от того, чем занимается армия.

Кто стоит за ботнетами? Иногда отдельные хакеры, но обычно это организованные преступные группы. Лучше с ними не сталкиваться! Говорят, что следующая война (на Земле, не в галактике) будет вестись в киберпространстве.

Вы хотите стать охотником на ботнеты? Есть специалисты, которые занимаются этим. Проблема в том, что в процессе выслеживания и обезвреживания ботнета Вы, возможно, нарушите некоторые законы. Лучше предоставить эту работу профессионалам. Они должны работать в рамках закона.

Ботнеты также используются для атак типа **«отказ в обслуживании» (denial of service, DoS)**. В ходе некоторых недавних DoS-атак хакеры требовали деньги в обмен на прекращение атаки. В прошлом большинство DoS-атак с помощью большого количества запросов данных пыталось вывести из рабочего состояния серверы сети или привести к перезагрузке системы. Некоторые ботнеты состоят из тысяч машин, которые проводят одну атаку на другую сеть для разрушения системы какой-либо организации и, как следствие, бизнеса.

Ботнеты — это отдельные компьютеры, расположенные по всему миру, но управляемые одним или несколькими серверами управления **(command and control (C&C) servers)**. Каждая машина управляется C&C-серверами и получает инструкции по тому, что и где атаковать. Сами C&C-серверы управляются другим, главным сервером (mothership). Когда между хакерами и атакуемыми машинами находятся несколько отдельных слоёв, через которые проходит связь, поиск ответственных за атаки людей становится трудным.

БЕСПЛАТНЫЙ СЫР В МЫШЕЛОВКЕ

Люди хотят получать свои любимые песни, телепередачи, фильмы и многое другое бесплатно. Задумайтесь! Как, по-Вашему, хакеры могут распространять вредоносное ПО? Один из эффективных методов распространения вредоносных программ (и создания сети ботов) — это прикрепление этих программ к чему-то, что все хотят получить бесплатно. Если Вы используете небезопасную ОС, то не отключайте антивирусную программу для ускорения работы.

Что такое антивирусные программы и какие другие меры противодействия могут помочь при защите от вредоносного ПО? Каждый год производители антивирусного ПО рекламируют свою продукцию как самую лучшую в решении вопроса выявления вирусов. Крупнейшие производители антивирусного ПО (Norton, McAfee, AVG и Kaspersky) оплачивают работу исследовательских организаций

(журналы, выпуски новостей, социальные медиа) для рекомендации своей продукции. На самом деле, одни из лучших программ находятся в открытом доступе и они бесплатны. Очень важно найти утилиты, которые подходят именно Вам, а не кому-то другому.

СПОСОБЫ ДОСТАВКИ

Очень немного людей целенаправленно устанавливают вредоносные программы на свои системы, поэтому авторам вредоносного ПО необходимо находить способы установки своих программ без ведома пользователя. Есть несколько методов, которые успешно применяются для установки программ без ведома владельца устройства. Среди лучших из них есть такие: переупаковка, обновления и прикреплённые объекты (SMS, электронные письма, веб-ссылки и другие вредоносные URL).

В переупаковке (repackaging) используется реальная легальная программа. Разработчики вредоносного ПО могут взять такую программу и добавить к ней свой вредоносный код или перекомпилировать код этой программы с включением в него полезной нагрузки. Для Google Play стоило больших трудов контролировать легальные программы для устройств Android. Поскольку большинство пользователей не обращают внимание на исходный размер правильной программы, то становится достаточно просто заменить хорошую копию на вредоносную.

Обновление программного обеспечения — ещё один вариант, которым могут воспользоваться разработчики вредоносного ПО для обмана пользователей и установки своих программ. Разработчик вредоносного ПО может «уговорить» пользователя к загрузке обновления некоторой программы на компьютер этого пользователя. Сообщение об обновлении выглядит как настоящее и даже может указывать ссылку URL на настоящий патч программы. Щелчок по ссылке на обновление или URL на самом деле загружает вредоносную программу, при этом сообщая пользователю, что его программа обновляется. Такие случаи происходили с Adobe, Microsoft, Java и некоторыми другими производителями.

Мы уже обсуждали прикреплённые файлы как метод распространения вредоносного ПО. Но веб-ссылки всё же остаются самым простым способом, с помощью которого вредоносные программы могут оказаться на компьютере. Плагины для браузеров для работы Javascript, Ajax, PHP, Flash, программ для просмотра PDF и других программ позволяют вредоносному ПО прокрадываться с вредоносных веб-страниц. Это значит, что Вы должны быть настороже и учитывать все возможные точки доступа.

Один из более интересных методов установки вредоносного ПО — это использование многоступенчатой атаки. Вредоносный код размещается на системе пользователя по частям, чтобы избежать обнаружения. Например, пользователь может натолкнуться на ссылку на веб-сайте или повреждённый вызов какой-либо функции веб-браузера с определённого веб-адреса. Это отдельное событие позволяет небольшой программе начать работать в фоновом режиме. Эта программа может провести некоторые изменения в настройках системы, открыв порт или обойдя некоторые средства защиты. После завершения этого этапа загружается другая программа; это может быть полезная нагрузка или вторая ступень атаки.

Этот многоступенчатый процесс загрузки программы может продолжаться столько, сколько необходимо для того, чтобы установить вредоносное ПО и провести атаку. Обычно вредоносное ПО с многоступенчатой загрузкой достаточно сложное, и оно может собирать информацию из больших наборов данных, таких как базы данных финансовых учреждений или базы данных кредитных карт. Атака на сеть американской фирмы Target в конце 2013 года

была многоступенчатой: в ходе атаки вредоносные программы обновлялись как минимум 5 раз.

Кроме обычных механизмов доставки файлов, некоторые разработчики для распространения вредоносного ПО используют встроенные в компьютер каналы связи. Например, программа **Flame** могла использовать Bluetooth для передачи вредоносного ПО на находящиеся рядом компьютеры. Wi-Fi также используется для передачи вредоносного кода. Говорят, что некоторые вредоносные программы для пересылки данных на другие устройства использовали высокочастотные звуковые тоны. Было доказано, что эта техника работает в лабораторных условиях, где наблюдается практически абсолютная тишина. Но не ждите, что это хорошо будет работать возле Вашего дома. Вы слишком громко разговариваете и храпите.

МЕРЫ ПРОТИВОДЕЙСТВИЯ

Существуют много методов определения и удаления вредоносного ПО; также есть много способов предотвращения его установки. В этом разделе представлено их краткое описание и примеры.

АНТИВИРУСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Сегодня существует множество антивирусных программ, как коммерческих, так и бесплатных. Они используют похожие методы. Каждая из них имеет базу данных известных вирусов; антивирусная программа сравнивает сигнатуры вирусов с файлами в системе, чтобы определить, есть ли какое-либо заражение (такой подход основывается на **чёрных списках (blacklist)**). Однако часто для современных вирусов эти сигнатуры очень маленькие, и результаты могут быть ложноположительными — файлы могут казаться вирусами, хотя на самом деле ими не являются.

Некоторые сканеры вирусов применяют **эвристики**, то есть сканеры имеют общее представление того, как ведёт себя вирус, и пытаются определить, соответствует ли неизвестное приложение этим критериям. Совсем недавно некоторые антивирусные программы позаимствовали принципы работы **хостовых систем обнаружения вторжений (Host-based Intrusion Detection)**, создавая список файлов и контрольных сумм для ускорения сканирования.

И да, компьютеры Mac фирмы Apple тоже подвержены воздействию вредоносного ПО. По текущим оценкам, существует около 5 тысяч разных видов вредоносных программ для устройств Apple. Существуют наборы эксплойтов, разработанных специально для атаки на Mac. Сейчас существует много антивирусных программ для Mac. Поищите в Интернете антивирусную программу для Mac.

Используете ли Вы антивирусные программы на своём iPhone или iPad? На своём телефоне Android или планшете? На своём телевизоре или плеере с доступом в Интернет? На своём Linux-box? Почему нет? Является ли антивирусное ПО обязательным?

По следующей ссылке Вы найдёте список бесплатных программ для решения проблем с вредоносным ПО: https://www.soldierx.com/tutorials/Malware-Removal-Guide.

УДАЛЕНИЕ НЕЖЕЛАТЕЛЬНЫХ ГОСТЕЙ

Некоторые вредоносные программы удалить легче, чем другие. Если Вы столкнулись с какими-либо неприятными вирусами, троянами или программами-вымогателями, то большинство антивирусных программ сможет удалить эти угрозы за несколько секунд. Существуют и другие виды вредоносного ПО, от которых избавиться не так просто и над удалением которых надо потрудиться; например, руткиты. Некоторые виды вредоносных программ практически невозможно удалить без повреждения данных в системе.

Первый шаг в процессе удаления нежелательного программного обеспечения — это идентификация вредоносной программы. Большинство антивирусных программ может определить название вредоносного ПО, и Вы уже самостоятельно сможете исследовать этот вид программы. Лучше иметь несколько разных антивирусных сканеров, поскольку одного никогда не бывает достаточно. После того, как Вы узнали название вредоносной программы, зайдите на сайт http://www.malwareremovalguides.info и прочитайте рекомендации по удалению этой угрозы.

Разные типы вредоносного ПО должны удаляться по-разному, поэтому исследуйте этот вопрос перед тем, как удалять файлы на компьютере.

Если на Вашем компьютере был обнаружен вирус, то, скорее всего, он там не один. Часто на одном компьютере можно обнаружить несколько десятков разных видов троянов. Разберитесь со всеми, начиная с самых сложных.

АНАЛИЗ ВРЕДОНОСНЫХ ПРОГРАММ

Представьте, что Вы работаете в компании по производству антивирусного ПО и Вы обнаружили новый вредоносный код, который раньше был неизвестен. Вам нужно будет оценить ущерб, который он может причинить, и определить его назначение, задокументировать и внести в каталоги новую вредоносную программу и (что самое важное) назвать её в свою честь. Только представьте себе!

По очевидным причинам будет неразумно запускать вредоносную программу на своём компьютере или на общем компьютере, подключённом к сети. Если Вы серьёзно заинтересованы анализом вредоносного ПО, то Вам нужно многое об этом узнать; Вам также понадобится тестовая система специально для этой цели. Сейчас достаточно просто написать свою вредоносную программу или найти в Интернете код вируса. Пожалуйста, будьте осторожны, проникая на «тёмную сторону» Интернета. Разработчики вредоносного ПО — это, прежде всего, люди, часто со злонамеренными и преступными умыслами; Вы не захотите проводить с ними время или приглашать их к себе домой.

При статическом анализе возможно изучить программу без её запуска. Для этого используются **дизассемблеры (disassemblers)**, **декомпиляторы (decompilers)** и **анализаторы исходного кода (source code analyzers).** Дизассемблирование программы заключается в преобразовании файла программы в листинг инструкций на машинном языке; декомпиляция программы — это преобразование инструкций на машинном языке в эквивалентный исходный код на языке более высокого уровня; а статический анализ — это исследование программы без её запуска.

Что если вредоносное ПО зашифровано? Если код зашифрован, Ваша задача немного усложняется, но остаётся разрешимой. Зашифрованный вредоносный код обычно является признаком того, что эта программа — это многоступенчатое приложение. Часть кода, которая должна расшифровать программу, уже может быть где-то на компьютере. Вам нужно будет поискать скрипт или приложение, которое было загружено приблизительно в то же время, когда была доставлена вредоносная программа.

Для обычных вредоносных программ стандартная процедура заключается в установке и запуске их на виртуальной машине. В зависимости от типа вредоносного ПО (исполняемый файл, приложение Java, скрипт или что-то другое), Вам необходимо будет декомпилировать программу в песочнице на виртуальной машине. Это задача не для слабонервных. Большинство вредоносных программ уже были декомпилированы и занесены в каталоги другими исследователями. Вы можете сохранить своё время и свои усилия, поискав эту информацию и используя её как дорожную карту.

Два примера сайтов для загрузки вредоносного ПО — это http://virusscan.jotti.org/en или https://www.virustotal.com/. На этих сайтах код анализируется популярными антивирусными программами, после чего Вы получаете результат анализа. Есть несколько пунктов, на которые следует обратить внимание. К ним относятся:

- **Распространение:** Как распространяется эта вредоносная программа
- **Заражение**: Как она устанавливается и почему не удаляется, несмотря на попытки удаления
- **Самозащита**: Как она скрывает своё присутствие и противостоит анализу
- **Возможности**: Какая функциональность доступна владельцу программы

Совет: никогда не доверяйте и не нажимайте на всплывающие окна, предлагающие бесплатную антивирусную программу, если в сообщении сказано, что Ваш компьютер заражён. Это почти всегда приманка вредоносной программы!

Помните, что расширение файла JAR — это сжатый файл Java (Java ARchive). Если Вам когда-нибудь захочется исследовать элементы Java, прочтите статью http://en.wikipedia.org/wiki/Decompiler или ознакомьтесь с проектом JAD по ссылке http://varaneckas.com/jad/.

УПРАЖНЕНИЯ

6.24 Найдите в Интернете **Sandboxie**. (Также не помешает поискать утилиты, похожие на Sandboxie.) На какой ОС используется эта утилита? Как она работает? С какими приложениями Вы бы её использовали?

6.25 Пользуетесь ли Вы бесплатными антивирусными программами? Конечно, Вы можете ими пользоваться, но давайте их проверим. Зайдите на веб-сайт производителя и найдите там сравнительную характеристику бесплатной и коммерческой версий (весьма вероятно, что такое сравнение есть). Какие отличия есть между этими версиями? Что Вы получите с приобретением полной версии?

6.26 Поищите в Интернете «сравнение антивирусных программ». Выберите текущий рейтинг (для текущего года). Какая антивирусная продукция находится на первом месте? Чем она отличается от других?

6.27 Теперь протестируйте свою антивирусную программу: определит ли она все угрозы на Вашем компьютере? Для начала зайдите на сайт бесплатного онлайн детектора вредоносных программ http://quickscan.bitdefender.com. Запустите онлайн-сканирование. Это может занять некоторое время, так что Вы можете заняться чем-то полезным, пока ждёте. Обнаружил ли Bitdefender какие-нибудь вредоносные программы, которые пропустила Ваша антивирусная программа? Если да, то почему Ваша антивирусная программа не обнаружила их?

6.28 Протестируйте свою антивирусную программу, используя поддельный вирус. Зайдите на веб-страницу http://www.eicar.org/anti_virus_test_file.htm и внимательно прочитайте раздел «Тестовый файл для антивирусных

программ и программ по поиску вредоносного ПО» («Antivirus or Anti-malware test file»). Файл, который Вы будете тестировать, на самом деле не является вирусом, но он создан таким образом, чтобы Вашей антивирусной программе казалось, что это вирус. Скачайте этот файл. Подождите, чтобы увидеть, что произойдёт. Что делает Ваша антивирусная программа? Закройте антивирусное сообщение (если оно появилось) и завершите процедуру загрузки.

6.29 Теперь откройте eicar_com.zip. Этот zip-файл содержит поддельный вирус. Что произошло, когда Вы попытались открыть этот файл? Определяет ли Ваша антивирусная программа этот файл как вредоносный?

6.30 Найдите в Интернета пример трояна и шпионской программы. Снова зайдите на сайт eicar.com.

6.31 Поищите в Интернете примеры руткитов и бэкдоров.

6.32 Теперь поразмышляйте: можете ли Вы поместить Ваш веб-браузер в песочницу, так что все загруженные файлы тоже попадут в песочницу? Является ли это эффективной альтернативой антивирусной программы?

NIDS/NIPS

Системы обнаружения вторжений в сеть (Network Intrusion Detection Systems, NIDS) похожи на антивирусные программы. Они ищут определённые сигнатуры или проявления поведения червей или вирусов. Они могут как просто предупреждать пользователя (как **системы обнаружения вторжений (Intrusion Detection System, IDS)**), или автоматически останавливать сетевой трафик, по которому передаётся вредоносное ПО (как системы **предотвращения вторжений (Intrusion Prevention System, IPS)**).

HIDS/HIPS

Хостовые системы обнаружения вторжений (Host-based Intrusion Detection systems, HIDS), такие как **Tripwire**, способны обнаруживать изменения файлов. Логично ожидать, что приложение после установки не должно изменяться, пока не будет обновлений; так что просмотр характеристик файла (например, его размер, дата последних изменений, контрольная сумма) сразу покажет, что что-то идёт не так.

БРАНДМАУЭРЫ

Черви распространяются по сети, используя уязвимости на каждом из хостов. Убедившись, что уязвимые службы не запущены, нужно удостовериться, что Ваш брандмауэр не разрешает установление соединений. Многие современные брандмауэры выполняют некоторую фильтрацию пакетов (аналогично HIPS) и отбрасывают пакеты, которые соответствуют определённой сигнатуре.

ПЕСОЧНИЦЫ

Концепция песочницы простая. У Вашего приложения есть свой собственный мирок для игры, и оно никак не может повлиять на другие процессы или программы в компьютере. Эта техника реализована как стандарт в языке программирования Java, и также может быть реализована с помощью других утилит, таких как **chroot** в Linux. Это ограничивает повреждения, которые может нанести операционной системе какая-либо вредоносная программа, которая требует доступ к чему-то и получает отказ. Во многих операционных системах такое ограничение всегда встроено. Но как минимум в одной ОС такого нет. (Попробуйте угадать, в какой.)

Другой вариант — работать на виртуальной машине (например, XEN или VirtualBox). Виртуальная машина изолируется от операционной системы, разрешая только тот доступ, который определён пользователем.

ПАТЧИ И РЕЗЕРВНОЕ КОПИРОВАНИЕ

Вот что говорит большинство производителей: применяйте каждый патч, применяйте все патчи, разрешите нам устанавливать все патчи, автоматически, всё время! Это обеспечит Вам безопасность!

Только нужно помнить о том, что:

1. Многие патчи, которые выпускают производители, не подходят именно для Вашей системы.
2. Каждый установленный Вами патч — это ещё более глючный код, который подвержен воздействию вредоносного ПО на Вашем компьютере.
3. Патчи ломают программы так же часто, как и чинят их.
4. Патчи могут вывести из строя или удалить другие стабильно работающие программы на Вашем компьютере или на сервере.

Другими словами, патчи нельзя назвать панацеей, как утверждают многие. Подходящие патчи обычно приносят пользу, хотя они могут и создавать новые проблемы. Но разрешение автоматических обновлений (многие админы узнали это на собственном опыте) действительно очень опасно. (Компания Microsoft оказала всем большую услугу, в очередной раз на своём примере показав нам это.)

Главное — это регулярно обновлять программное обеспечение, но при этом тестировать патчи перед установкой их на важных машинах. Если Вы не можете протестировать патч, убедитесь, что Вы сможете отменить его установку. Облачные хранилища данных с каждым днём становятся дешевле, и Вы можете установить автоматическое резервное копирование и синхронизацию данных между Вашим компьютером и учётной записью. Не забывайте о локальном добавочном резервном копировании. Ваши данные имеют ценность, храните их надёжно.

ШИФРОВАНИЕ

Полное шифрование диска — ещё одна хорошая идея для защиты Ваших данных и Вашей системы от вредоносного ПО. Бесплатные программы могут обеспечить превосходное шифрование, в то же время оставляя работу на компьютере удобной для пользователя. Одна из особенностей применения шифрования диска — это то, что оно заменяет загрузочный сектор на диске своей собственной начальной загрузкой. Это снижает риск появления руткитов и заражения загрузочного сектора вредоносными программами.

Вредоносный код не может атаковать то, что он не может увидеть. Зашифрованные файлы сохраняют секретную информацию под Вашим контролем, так что она не будет отправлена оператору вредоносной программы. Это ограничивает возможность вредоносного ПО получить доступ к таким ценным данным, как пароли, подробные данные о банковском счёте, отчёты и фотографии, которые Вы не хотели бы никому показывать.

Зашифруйте не только Ваш жёсткий диск. Зашифруйте все носители и Ваш телефон.

УПРАЖНЕНИЯ

6.33 В поисковой системе задайте запрос «автоматическое обновление стало причиной». Сколько неприятностей может случиться из-за автоматических обновлений? Сколько результатов Вы получили?

6.34 Исследуйте антивирусные программы для мобильных телефонов. Также поищите программы против вредоносного ПО для планшетов (например, iPad и Android). Эффективны ли эти утилиты? Кто пользуется ими?

6.35 Исследуйте Stuxnet, Duqu и Flame. Для каждого из них ответьте на вопросы:

- На какие системы он воздействовал?
- Какая была его полезная нагрузка?
- Чем эта программа отличается от других вредоносных программ?
- Как удалить их из системы?

6.36 Игра «Подбери пару»: Исследуйте каждый из следующих продуктов и подберите для них пару — к какому типу мер противодействия они принадлежат:

http://www.virtualbox.org	NIDS/NIPS
http://www.tripwire.org	Антивирус
http://www.snort.org	Брандмауэр
http://www.checkpoint.com	Песочница
http://www.clamav.net	HIDS/HIPS

6.37 Исследуйте, как работают NIDS/NIPS и HIDS/HIPS.

6.38 Поищите в Интернете информацию о брандмауэрах. Вы можете анализировать журналы брандмауэров и загружать их на сайт SANS Internet Storm Center, DShield по ссылке http://isc.sans.edu/howto.html.

6.39 Поищите в Интернете информацию о **chroot**. Почитайте об этом типе «тюрьмы» или «песочницы».

6.40 Нарисуйте **дерево атак (Attack Tree)**. Выполните расширенный поиск по "site:www.schneier.com."

6.41 Вредоносные программы приносят пользу только тем, кто получает с их помощью прибыль и рискует быть пойманным. Все хотят избежать заражения вредоносным ПО. Посмотрите на схему по ссылке http://www.computerschool.org/computers/malware/ («Бизнес вредоносного ПО», «Inside the business of malware»), чтобы понять, чего именно Вы избегаете, защищаясь от вредоносного ПО.

6.42 На сайте computerschool.org есть инфографика «Бизнес вредоносного ПО» (Business of Malware). Найдите её.

ЗАКЛЮЧЕНИЕ

Основой хорошей защищённости от вредоносных программ является хорошее понимание этих вредоносных программ. Мы не можем охватить все возможные типы вредоносного ПО (поскольку, пока Вы читаете этот текст, появляются всё новые программы), но мы осветили некоторые наиболее важные темы. Например, Вы едва можете доверять ярлыкам на рабочем столе Вашего компьютера и Вам совсем не следует доверять каким-либо файлам, которые Вы не запрашивали. Ключевым моментом является доверие, которое зависит от хорошей осведомлённости о том, насколько уязвимыми Вы становитесь, проявляя это доверие.

Мы не хотим, чтобы Вы стали абсолютно недоверчивыми ко всему; такое отношение оградит Вас от множества возможностей. Просто помните, что, предоставляя кому-либо доступ к своим данным, Вы доверяете им. Принципы, которые делают работу в сети безопасной, также могут сделать безопасной Вашу жизнь. Например, сегментация, которая допускает только тесно управляемую видимость, — это эффективный метод как в работе в сети, так и в реальной жизни.

Мы также не поощряем того, чтобы Вы занимались разработкой вредоносного ПО и испытанием его на компьютерах знакомых или незнакомых Вам людей. Теперь (возможно, более, чем когда-либо в истории человечества) действия имеют свои последствия. Не сомневайтесь — мы могли бы найти Вас, если бы попытались; и мы далеко не такие страшные, как некоторые представители власти или правоохранительных органов.

Вместо этого мы хотим, чтобы Вы увидели, как работает вредоносное ПО и какие существуют схемы мошенничества. Это обезопасит Вас не только от вредоносных программ, но и в целом от неприятностей в жизни.

Используй эту силу только во благо, юный падаван.

Today's teens are in a world with major communication and productivity channels open to them and they don't have the knowledge to defend themselves against the fraud, identity theft, privacy leaks and other attacks made against them just for using the Internet. This is the reason for Hacker Highschool.

The Hacker Highschool project is the development of security and privacy awareness learning materials for junior high and high school students.

Hacker Highschool is a set of lessons and a practical means of making hackers. Beyond just providing cybersecurity awareness and critical Internet skills, we need to teach the young people of today how to be resourceful, creative, and logical, traits synonymous with hackers. The program contains free security and privacy awareness teaching materials and back-end support for teachers of accredited junior high, high schools, and home schooling. There are multiple workbooks available in multiple languages. These are lessons that challenge teens to be as resourceful as hackers, including safe Internet use, web privacy, researching on the internet, avoiding viruses and Trojans, legalities and ethics, and more.

The HHS program is developed by ISECOM, a non-profit, open-source research group focused on security awareness and professional security development and accreditation.

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM