ВикипедиЯ

Сетевой червь

Материал из Википедии — свободной энциклопедии

Сетевой червь — разновидность вредоносной программы, самостоятельно распространяющейся через локальные и глобальные (Интернет) компьютерные сети.

Содержание

История

Ранние эксперименты по использованию компьютерных червей в распределённых вычислениях были проведены в исследовательском центре Xerox в Пало-Альто Джоном Шочем (John Shoch) и Йоном Хуппом (Jon Hupp) в 1978 году. Термин «червь» возник под влиянием научно-фантастических романов «Когда ХАРЛИ исполнился год» Дэвида Герролда (1972), в котором были описаны червеподобные программы, и «На ударной волне» Джона Браннера (1975), где вводится сам термин.

Одним из наиболее известных компьютерных червей является «Червь Морриса», написанный в 1988 г. Робертом Моррисом-младшим, который был в то время студентом Корнеллского Университета. Распространение червя началось 2 ноября, после чего червь быстро заразил примерно 6200 компьютеров (это около 10 % всех компьютеров, подключённых в то время к Интернету).

Механизмы распространения

Все механизмы («векторы атаки») распространения червей делятся на две большие группы:

- Использование уязвимостей и ошибок администрирования в программном обеспечении, установленном на компьютере. Червь Морриса использовал известные на тот момент уязвимости в программном обеспечении, а именно в почтовом сервере sendmail, сервисе finger и подбирал пароль по словарю. Такие черви способны распространяться автономно, выбирая и атакуя компьютеры в полностью автоматическом режиме.

- Используя средства так называемой социальной инженерии, провоцируется запуск вредоносной программы самим пользователем. Чтобы убедить пользователя в том, что файл безопасен, могут подключаться недостатки пользовательского интерфейса программы — например, червь VBS.LoveLetter использовал тот факт, что Outlook Express скрывает расширения файлов. Данный метод широко применяется в спам-рассылках, социальных сетях и т. д.

Иногда встречаются черви с целым набором различных векторов распространения, стратегий выбора жертвы, и даже эксплойтов под различные операционные системы.

Скорость распространения

Скорость распространения сетевого червя зависит от многих факторов: от топологии сети, алгоритма поиска уязвимых компьютеров, средней скорости создания новых копий.

Для сетевых червей, распространяющихся по сети путём непосредственного использования протоколов TCP/IP, то есть, с любого IP-адреса на любой другой, характерно стремительное распространение. При условии, что каждый экземпляр червя достоверно знает адрес ранее незараженного узла сети, возможно экспоненциальное размножение. Например, если каждый экземпляр заражает один компьютер в секунду, все адресное пространство IPv4 будет заполнено червем за полминуты. Гипотетический червь, который был бы способен распространяться с такой скоростью, получил наименование «блицкриг-червя». Исследователем Н.Уивером из университета Беркли рассмотрены несложные субоптимальные алгоритмы, которые могли бы позволить червю, размножаясь несколько медленнее, тем не менее заразить Интернет за 15 минут. Червь такого типа получил наименование «червь Уорхола» — в честь Энди Уорхола, автора изречения:

> *В будущем каждый получит шанс на 15 минут славы*

Эпидемия червя SQL Slammer, заразившего в 2003 г. более 75000 серверов за 10 минут, была близка к этой модели распространения.

Тем не менее, подавляющее большинство червей использует гораздо менее эффективные алгоритмы. Экземпляры типичного червя ищут уязвимые узлы сети методом проб и ошибок — случайным образом. В этих условиях кривая его размножения соответствует решению дифференциального уравнения Ферхюльста и приобретает «сигмовидный» характер. Корректность такой модели была подтверждена в 2001 году во время эпидемии червя CodeRed II. За 28 часов червь заразил около 350 000 узлов сети, причем в последние часы скорость его распространения была довольно мала — червь постоянно «натыкался» на ранее уже зараженные узлы.

В условиях активного противодействия со стороны антивирусов, удаляющих экземпляры червя и вакцинирующих систему (то есть делающих её неуязвимой), кривая эпидемии должна соответствовать решению системы уравнений Кермака-Маккендрика с острым, почти экспоненциальным началом, достижением экстремума и плавным спадом, который может продолжаться неделями. Такая картина, действительно, наблюдается в реальности для большинства эпидемий.

Вид кривых размножения для червей, использующих почтовые протоколы (SMTP), выглядит примерно так же, но общая скорость их распространения на несколько порядков ниже. Связано это с тем, что «почтовый» червь не может напрямую обратиться к любому другому узлу сети, а только к тому, почтовый адрес которого присутствует на зараженной машине (например, в адресной книге почтового клиента Outlook Express). Продолжительность «почтовых» эпидемий может достигать нескольких месяцев.

Структура

Черви могут состоять из различных частей.

Часто выделяют так называемые резидентные черви, которые могут инфицировать работающую программу и находиться в ОЗУ, при этом не затрагивая жёсткие диски. От таких червей можно избавиться перезапуском компьютера (и, соответственно, сбросом ОЗУ). Такие черви состоят в основном из «инфекционной» части: эксплойта (шелл-кода) и небольшой полезной нагрузки (самого тела червя), которая размещается целиком в ОЗУ. Специфика таких червей заключается в том, что они не загружаются через загрузчик, как все обычные исполняемые файлы, а значит, могут рассчитывать только на те динамические библиотеки, которые уже были загружены в память другими программами.

Также существуют черви, которые после успешного инфицирования памяти сохраняют код на жёстком диске и принимают меры для последующего запуска этого кода (например, путём прописывания соответствующих ключей в реестре Windows). От таких червей можно избавиться только при помощи антивирусного программного обеспечения или подобных инструментов. Зачастую инфекционная часть таких червей (эксплойт, шелл-код) содержит небольшую полезную нагрузку, которая загружается в ОЗУ и может «догрузить» по сети непосредственно само тело червя в виде отдельного файла. Для этого некоторые черви могут содержать в инфекционной части простой TFTP-клиент. Загружаемое таким способом тело червя (обычно отдельный исполняемый файл) теперь отвечает за дальнейшее сканирование и распространение уже с инфицированной системы по локальной сети, а также может содержать более серьёзную, полноценную полезную нагрузку, целью которой может быть, например, нанесение какого-либо вреда (к примеру, DoS-атаки).

Большинство почтовых червей распространяются как один файл. Им не нужна отдельная «инфекционная» часть, так как обычно пользователь-жертва при помощи почтового клиента или Интернет-браузера добровольно скачивает и запускает червя целиком.

Полезная нагрузка (Payload)

Зачастую черви даже безо всякой полезной нагрузки перегружают и временно выводят из строя сети только за счёт интенсивного распространения. Типичная осмысленная полезная нагрузка может заключаться в порче файлов на компьютере-жертве (в том числе, изменение веб-страниц, так называемый «deface»), также из зараженных компьютеров возможна организация ботнета для проведения сетевых атак, рассылки спама или майнинга криптовалют.

Способы защиты

По причине того, что сетевые черви для своего проникновения в систему пользователя используют уязвимости в стороннем программном обеспечении или операционной системе, использования сигнатурных антивирусных мониторов недостаточно для защиты от червей. Также, при использовании методов социальной инженерии пользователя под благовидным предлогом вынуждают запустить вредоносную программу, даже несмотря на предупреждение со стороны антивирусного программного обеспечения. Таким образом, для комплексного обеспечения защиты от современных червей, и любых других вредоносных программ, необходимо использование проактивной защиты. Рассматривается также способ защиты от сетевых червей на основе «кредитов доверия». Ряд преимуществ дает применение межсетевых экранов и подобных им утилит (например, Windows Worms Doors Cleaner)

См. также

- Хронология компьютерных вирусов и червей
- Многовекторный червь

Примечания

Ссылки

- Климентьев К. Е. Компьютерные вирусы и антивирусы: взгляд программиста. — М.: ДМК-Пресс, 2013. С. 656. ISBN 978-5-94074-885-4
- John Shoch, Jon Hupp The 'Worm' Programs — Early Experience with a Distributed Computation" (https://web.archive.org/web/20051029161448/http://vx.netlux.org/lib/ajm01.html) (англ.), Communications of the ACM, March 1982 Volume 25 Number 3, pp. 172—180, ISSN 0001—0782
- Nicholas C. Weaver Warhol Worms: The Potential for Very Fast Internet Plagues (http://www.iwar.org.uk/comsec/resources/worms/warhol-worm.htm)
- RFC 1135 (англ.)— The Helminthiasis of the Internet