

Основные виды компьютерных вирусов

Вирусы черви

Черви создают копии самих себя. Их опасность в захламлении ПК, из-за чего его производительность существенно снижается. Особенность червяков, как компьютерных вирусов в том, что они попадают в ОС, используя ее уязвимости. Вирусы распространяются по сетям и поражают не только отдельные программы, но и целые системы. В этом отличие компьютерных червей от других вирусов. Объектами их нападения могут стать даже правительственные информационные системы.

Трояны

Компьютерные вирусы Трояны прячутся в безвредных программах. Они неопасны, пока пользователь их не запустит. Поэтому их сложно выявить до начала активной деятельности. Компьютерные вирусы Трояны наносят существенный вред ПК. Чаще всего используются для кражи, удаления или замены персональной информации. Самостоятельно размножаться они не могут до того момента, пока жертва сама не впустит «коня» в систему.

Компьютерные вирусы Зомби

Виды компьютерных вирусов, позволяющие хакерам управлять устройствами без разрешения их владельцев. При попадании в ПК они могут долго себя не проявлять, пока не поступит команда от управляющей программы. Она «будит» вирус и он начинает атаки, которые заключаются в нанесении вреда системе или рассылке спама. Заражение ПК идет постепенно, до тех пор, пока в компьютере не будет нужный объем вирусов Зомби для поражения запланированных целей. Вредоносное ПО способно атаковать крупные компании, сети различных предприятий и организаций.

Руткиты

Специальные маскировщики, цель которых – сокрытие деятельности других вирусов и активности преступников. Для этого руткиты используют разные ухищрения. Например, изменяют работу ОС, отключают или запускают различные функции, блокируют антивирусники, чтобы они не нашли внутри ПК замаскированное ПО.

Логические бомбы

Логическая бомба – это не вирус для компьютера в прямом понимании, а кусок кода, внедренный в программу. Код работает при выполнении заданных параметров. Например, злоумышленник может его вставить в любое расширение браузера. Он запускается при каждом открытии стартовой страницы. Запоминает нажатия клавиш, чтобы украсть пароли, логины и другую информацию для входа на финансовые и прочие сервисы.

Логистические бомбы вставляются в действующее ПО или другие вирусные продукты. Они находятся в спящем режиме и могут долго не замечаться антивирусниками.

Бэкдор вирусы (Backdoor)

Программы, которые ставятся хакерами на взломанные устройства после получения первого доступа для возможности повторного проникновения в систему. Назначение Backdoor – обеспечение скрытого управления оборудованием. Вирус позволяет копировать данные, передавать их на чужие ПК и другие устройства. Помогает получать доступы к реестрам и выполнять системные транзакции. Например, перезагружать ПК, модифицировать пароли, создавать новые сетевые ресурсы и т.д.

Многие черви содержат в себе Backdoor. Вирусы позволяют хакерам использовать зараженные девайсы для сканирования сетей, взлома и атак.

Эксплойт (Exploit)

Вирус также позволяет хакеру подключаться к чужому ПК, но не дает управлять им, поэтому считается менее вредоносным. Однако он способствует проникновению более опасных вредителей. Вирус ищет уязвимости системы для получения прав администратора или нагружает ее, чтобы нарушить функциональность (DDoS атака).

Загрузочные вирусы

Поражают запись MBR и секторы хранения данных. Вписывают код в таблицу разделов винчестера. После новой загрузки ПК они проникают в основную память. За счет качественной шифровки их сложно выявить и удалить. Вирусы нарушают процесс загрузки, делают работу ОС нестабильной, блокируют жесткие диски.

Программы шпионы (Spyware)

Основная цель таких вирусов – кража данных из памяти. Например, логинов, паролей, сведений о банковских картах и т.д. Вся собранная информация направляется на сервер, отмеченный хакером. Вирусы могут долгое время оставаться незамеченными из-за отсутствия активности, поэтому их также сложно выявлять и обезвреживать.

Скрипт вирусы (Script)

Вредители живут в Интернете. При посещении зараженного сайта браузер пользователя загружает и запускает вредоносный код. Сам по себе он безвредный, но может содержать более опасные вирусы. Ссылки на вирусные страницы рассылаются в сообщениях через E-mail или мессенджеры.

Вирусы влияют на работу браузеров, меняют настройки и захватывают их, позволяя хакерам делать изменения в веб-страницах на стороне клиента. В основном они направлены на сайты соцсетей. Некоторые способны инициировать DDoS-атаки, чтобы сделать функционирование серверов максимально медленным.

Мутанты

Компьютерные вирусы мутанты содержат алгоритмы шифрования и расшифровки, за счет которых копии одной и той же программы не имеют одинаковых цепочек

байтов. Их трудно выявить из-за сложных алгоритмов и модификаций. Все последующие версии мутирующего вируса имеют более развитый функционал и не похожи на своего родителя. Вирус мутант может нанести существенный вред компьютеру.