ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ «БОРОВИЧЕСКИЙ АВТОМОБИЛЬНО-ДОРОЖНЫЙ КОЛЛЕДЖ»

ТЕМА: Защита пк от вирусов Антивирусные средства

Студент Гучас Л.А.

Боровичи

2018

Антивирусная программа

Антивирусная программа— специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ и восстановления заражённых (модифицированных) такими программами файлов, а также для профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.

Задачи антивируса

Основными задачи, которые ставятся перед программным антивирусным обеспечением, являются:

1. препятствие проникновения зараженной информации в компьютерную систему;
2. минимизация последствий от вирусов;
3. обнаружение источника вируса;
4. удаление и нейтрализация вредоносных файлов.

Антивирусная база – это основа, где хранятся сигнатуры вирусов. Эта база данных нуждается в периодическом обновлении, чтобы поддерживать актуальность антивируса.

Методы защиты от вирусов

Для защиты от вирусов используют три группы методов:

1. Методы, основанные на *анализе содержимого файлов* (как файлов данных, так и файлов с кодами команд). К этой группе относятся сканирование сигнатур вирусов, а также проверка целостности и сканирование подозрительных команд.
2. Методы, основанные на *отслеживании поведения программ* при их выполнении. Эти методы заключаются в протоколировании всех событий, угрожающих безопасности системы и происходящих либо при реальном выполнении проверяемого кода, либо при его программной эмуляции.
3. Методы *регламентации порядка работы* с файлами и программами. Эти методы относятся к административным мерам обеспечения безопасности.

Специальные антивирусы

В ноябре 2014 года международная правозащитная организация Amnesty International выпустила антивирусную программу Detect, предназначенную для выявления вредоносного ПО, распространяемого государственными учреждениями для слежки за гражданскими активистами и политическими оппонентами. Антивирус, по заявлению создателей, выполняет более глубокое сканирование жёсткого диска, нежели обычные антивирусы.

Лжеантивирусы

В 2009 началось активное распространение лжеантивирусов — программного обеспечения, не являющегося антивирусным (то есть не имеющего реальной функциональности для противодействия вредоносным программам), но выдающим себя за таковое. По сути, лжеантивирусы могут являться как программами для обмана пользователей и получения прибыли в виде платежей за «лечение системы от вирусов», так и обычным вредоносным программным обеспечением.

Эффективность антивирусов

- Аналитическая компания Imperva в рамках проекта Hacker Intelligence Initiative опубликовала интересное исследование[5][6], которое показывает малую эффективность большинства антивирусов в реальных условиях.

- По итогам различных синтетических тестов антивирусы показывают среднюю эффективность в районе 97 %, но эти тесты проводятся на базах из сотен тысяч образцов, абсолютное большинство которых (может быть, около 97 %) уже не используются для проведения атак.

- Вопрос в том, насколько эффективными являются антивирусы против самых актуальных угроз. Чтобы ответить на этот вопрос, компания Imperva и студенты Тель-Авивского университета раздобыли на российских подпольных форумах 82 образца самого свежего вредоносного ПО — и проверили его по базе VirusTotal, то есть против 42 антивирусных движков. Результат оказался плачевным.

1. Эффективность антивирусов против только что скомпилированных зловредов оказалась менее 5 %. Это вполне логичный результат, поскольку создатели вирусов обязательно тестируют их по базе VirusTotal.
2. От появления вируса до начала его распознавания антивирусами проходит до четырёх недель — это у «элитных» антивирусов, а у остальных срок может доходить до 9-12 месяцев. Например, в начале исследования 9 февраля 2012 года был проверен свежей образец фальшивого инсталлятора Google Chrome. После окончания исследования 17 ноября 2012 года его определяли только 23 из 42 антивирусов.
3. У антивирусов с самым высоким процентом определения зловредов присутствует также высокий процент ложных срабатываний.
4. Хотя исследование сложно назвать объективным, ибо выборка зловредов была слишком маленькой, но можно предположить, что антивирусы совершенно непригодны против свежих киберугроз.

Заключение

Заключение Наверное, большинство пользователей уже поняло, что антивирус – это программа для полной защиты не только от вирусов, но и от множества сторонних угроз, связанных со шпионажем или с кражей конфиденциальной информации, в общем, от всего, что может представлять собой угрозу для операционной системы, «железа» (есть и такие вирусы) и пользовательских файлов, которые хранятся на винчестере, съемном носителе или даже в «облачном» хранилище.

Литература

- Язов Ю. К., Соловьев С. В. Защита информации в информационных системах от несанкционированного доступа. Пособие. — Воронеж: Кварта, 2015. — С. 357. — 440 с. — 232 экз. — ISBN 978-5-93737-107-2.
- Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. — 4-е изд. — СПб.: Питер, 2010. — С. 871-875. — 944 с. — 4500 экз. — ISBN 978-5-49807-389-7.
- Информационное сообщение ФСТЭК России Об утверждении требований к средствам антивирусной защиты от 30 июля 2012 г. № 240/24/3095 (рус.). Официальный сайт ФСТЭК России. fstec.ru (30 июля 2012). Проверено 20 января 2018.