ВИРУСЫ ШИФРОВАЛЬЩИКИ И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Работа
Учеников 11а класса
ГБОУСОШ №208
Даниловой Аси, Дороша Андрея
и Баранца Давида.

ОГЛАВЛЕНИЕ:

ВИРУСЫ ШИФРОВАЛЬЩИКИ

В нашей всемирной, глобальной системе под названием ИНТЕРНЕТ, существует огромное, мы бы сказали, нереально большое кол-во различных видов вирусов, но мы хотим привлечь ваше внимание к одному из самых “скрытных” вирусов, о которых вы, очевидно, мало слышали, в отличии от так называемых “троянов” “баннеров” и т.п. Собственно, это – вирусы шифровальщики.

Шифрованные вирусы (Encrypted viruses) - вирусы, которые сами шифруют свой код для затруднения их дезассемблирования и обнаружения в файле, памяти или секторе. Каждый экземпляр такого вируса будет содержать только короткий общий фрагмент - процедуру расшифровки который можно выбрать в качестве сигнатуры. В случае каждого инфицирования он автоматически зашифровывает себя, и каждый раз по-разному.

Такое вот сложное, заумное определение мы нашли в интернете, но, прочитав его, вы, очевидно, да и мы в частности, не смогли бы понять, что же это за особый вид вируса и с чем же его, всё-таки, кушают.

ВИРУСЫ ШИФРОВАЛЬЩИКИ

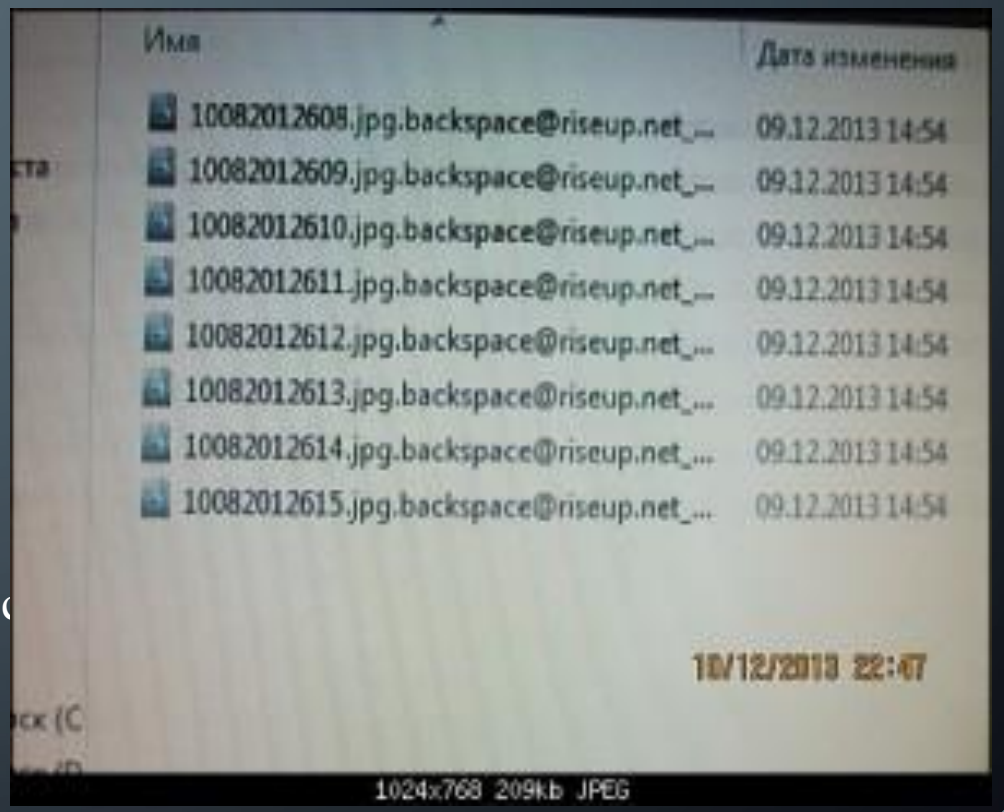
Давайте назовём наши страшные ШИФРОВАННЫЕ вирусы (само слово шифр уже звучит довольно сложно) как-нибудь по другому, к примеру – “подозрительные упаковщики” . Теперь попытаемся понять, что же они из себя представляют:

Чтобы предотвратить реконструкцию вредоносных программ и затруднить анализ поведения программ, разработчики вредоносного ПО (вируса) могут сжимать (или упаковывать) свои вредоносные программы различными способами, сочетая это с шифрованием файлов. Антивирусные программы обнаруживают результат работы подозрительных упаковщиков, но, говоря простыми словами, из-за многократного упаковывания (сжатия) антивирус думает, что он смог дойти до самого эпицентра событий, до самого вируса, но зачастую, кол-во алгоритмов шифрования, превышает способности антивируса, и он удаляет только часть этого самого шифра, не доходя, собственно до самой вирусной программы.

ВИРУСЫ ШИФРОВАЛЬЩИКИ

Теперь, когда мы хотя бы немножечко понимаем, как работает сам механизм нашего злого вируса, мы объясним вам, как работает его “замысел”

После попадания на компьютер вирус начинает шифровать практически всю ценную
информацию.
Зашифровываются: фотографии, различные документы, видео, сохраненные файлы программ итд. После окончания работы вируса, как правило, на рабочем столе компьютера остаются сообщения о проникновении и зашифровке, а также контактый E-mail для обратной связи с вымогателями-создателями вируса.
Для расшифровки файлов требуется программа-дешифратор, которую вымогатели “обязуются“ прислать за деньги.



ВИРУСЫ ШИФРОВАЛЬЩИКИ

И НАКОНЕЦ, САМЫЙ ТРЕВОЖНЫЙ МОМЕНТ-НЕТ НИ ОДНОГО АНТИВИРУСА, КОТОРЫЙ С ГАРАНТИЕЙ МОЖЕТ ЗАЩИТИТЬ КОМПЬЮТЕР ОТ ПРОНИКНОВЕНИЯ ДАННОГО ВИДА ВИРУСОВ, А ЭТО ЗНАЧИТ, ЧТО ВЕРОЯТНОСТЬ ЛИШИТЬСЯ ВСЕХ ЦЕННЫХ ДАННЫХ РАЗОМ, ЕСТЬ У КАЖДОГО ПОЛЬЗОВАТЕЛЯ КОМПЬЮТЕРА.

БОРЬБА С ВИРУСАМИ

Теперь нам стало интересно: реально ли защититься от вирусов на все 100% ? Об этом мы поговорим позже, а пока:

КАК ЖЕ НАМ ЗАЩИТИТЬ информацию и свой любимый компьютер от вирусов

БОРЬБА С ВИРУСАМИ

Резервное копирование

Несомненно, самым ЛУЧШИМ и ЭФФЕКТИВНЫМ средством защиты личных данных, которые хранятся на вашем компьютере, является резервное копирование.

БОРЬБА С ВИРУСАМИ

ПОЛНОЕ РЕЗЕРВНОЕ КОПИРОВАНИЕ (FULL BACKUP)

Полное копирование обычно затрагивает всю систему и все файлы. Еженедельное, ежемесячное и ежеквартальное резервное копирование подразумевает создание полной копии всех данных. Обычно оно выполняется тогда, когда копирование большого объёма данных не влияет на работу. Последующие резервные копирования, выполняемые до следующего полного копирования, могут быть, главным образом для того, чтобы сохранить время и место на носителе.

На наш взгляд, если информация, хранящаяся на вашем ПК, вам не просто дорога, а жизненно необходима (работа, учёба и др.) , то следует использовать именно FULL BACKUP, в противном случаи, вы сильно затруднитесь с восстановлением файлов. (но это подходит больше для организаций, компаний и тд)

БОРЬБА С ВИРУСАМИ

Резервное копирование в виде образа

Видов резервного копирования существует довольно большое кол-во, но последний, о котором мы расскажем вам: **Резервное копирование в виде образа**

Образ — точная копия всего раздела или носителя (устройства), хранящаяся в одном файле.

Иными словами, это самый мобильный и удобный способ хранения данных, т.к. ваша (сжатая) информация будет храниться всего в 1 файле, не требующего большого затрата места (объёма памяти)

К примеру вы можете сделать резервную копию в виде образа, затем скопировать его (образ) , например, на внешний носитель памяти (флеш карту.

Всё, небольшая трата времени и вы спите спокойно, не волнуясь за свои данные.

БОРЬБА С ВИРУСАМИ

Выбор антивируса

Далее, о чём хотелось бы упомянуть, это, конечно, выбор антивируса. Мы не можем спорить, какой антивирус будет лучше, а какой хуже, да и речь совсем не об этом.

А суть заключается в одном: ВСЕ пользователи должны понимать, что они просто “обязаны” иметь на своём ПК антивирус.

Но выбрать его (антивирус) всё же нужно, ведь иметь на компьютере больше 1-ого антивируса не рекомендуется, т.к. они будут мешать друг другу. Лично мы остановимся на совсем обычном критерии – удобство. Наш совет прост: попользуйтесь всеми антивирусами в бета версиях, чтобы понять, какой вам “по душе” , после чего вы сможете определиться, какой из них будет служить вам и вашему ПК долгое время.

ЗАЩИТА НАДЁЖНА ИЛИ ЖЕ НЕТ ???

Как мы уже смогли убедиться, полностью защититься от вирусов мы не можем, и доказательством является наш страшный вирус, о котором мы упомянули ранее, под названием “шифровальщик”.

Это, пожалуй, неоспоримый факт, НО защититься мы не можем в режиме “реального времени” , т.е. не можем избежать попадания вируса на наш компьютер!

Однако 100% -ый способ сохранить все файлы, хранящиеся на вашем ПК – ЕСТЬ

Как вы уже догадались это способ под названием:

РЕЗЕРВНОЕ КОПИРОВАНИЕ

НЕ ЛЕНИТЕСЬ, СОЗДАТЬ РЕЗЕРВНУЮ КОПИЮ НЕ ТРУДНО И ЗАЙМЁТ ЭТО НЕ БОЛЕЕ ЧАСА!!!
ВЕЛИКИЙ ГУГЛ ВАМ В ПОМОЩЬ.

ДА БУДУТ В СОХРАННОСТИ ВАШИ ФАЙЛЫ!!!

"Презентация подготовлена для конкурса "Интернешка" http://interneshka.org/".

СПАСИБО ЗА ВНИМАНИЕ