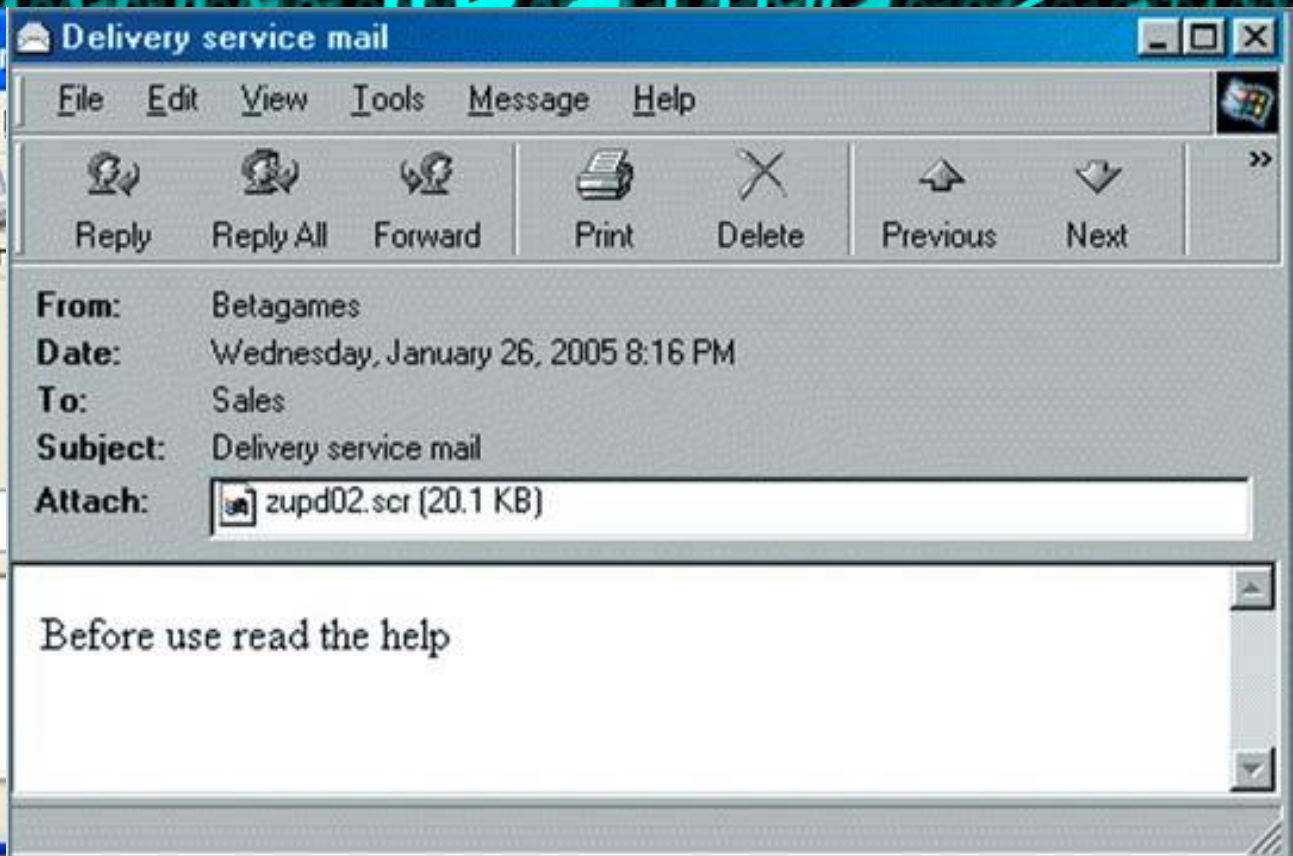
Вирус Bagle.AM

Составил: Ревнивцев М.В ; Преподователь: Кленина В.И

Вирус Bagle был еще одним вариантом классического вредоносного ПО для массовой спам-рассылки, но значительно модернизированным. Впервые был обнаружен в 2004 привычно заражал компьютеры пользователей через вложение к электронному письму, также использовал электронную почту для распространения. В отличие от предыдущих спам-вирусов, Bagle не полагался на адресную книгу почтовой программы MS Outlook, чтобы составить список адресатов, по которому можно разослать себя же. Он собирал все адреса электронной почты из различных документов, хранящихся в файлах на зараженном компьютере, — от обычных текстовых файлов до электронных таблиц MS Excel.

Письма рассылаемые вирусом Bagle



Особая опасность данного вредоноса состояла в том, что на пораженном компьютере он открывал черный ход, через который удаленный пользователь, вероятно, автор или группа хакеров, мог получить доступ и контроль над зараженным компьютером. Эта лазейка помогала загрузить дополнительные компоненты либо программу-шпион для кражи информации у пользователей или запустить DDoS-атаку на определенные сети и компьютеры. Хотя оригинальный вирус Bagle прекратил распространение после января 2004 г., сегодня сотни вариантов и разновидностей этого вируса все еще имеют хождение по Сети.

Серверы, где размещен вирусный модуль, находятся в разных местах планеты - вероятно, модуль был помещен на них в результате взлома. В индустриально развитых странах держатели таких серверов, как правило, быстро принимают меры и удаляют вредоносные компоненты, однако в развивающихся странах на "бесхозных" серверах меры могут приниматься долго, или вообще не приниматься - это позволяет вирусу распространяться далее.

Традиционно, пользователям рекомендуется не открывать вложения к подозрительным письмам (в данном случае - пустым, даже если отправителем значится знакомый человек или организация) и обновить антивирусные средства. Кроме того, зараженные письма с большой вероятностью будут отфильтрованы почтовыми серверами, где установлено антивирусное серверное ПО.

В 2004 Микко Гиппонен, директор по антивирусным исследованиям компании F-Secure, заявил, что исходный код подлинный, а тот факт, что он написан на чистом ассемблере, свидетельствует о том, что мы имеем дело не со script kiddie, а с серьезным программистом. Цитата: «Большинство червей пишут на языке C или частично на C и частично на ассемблере. Осталось не так много людей, хорошо знающих ассемблер, так что за этим стоит серьезный программист».

Гиппонен говорил, что хотя ассемблер — трудный язык, для мастера не составит труда модифицировать код и создать новые варианты Bagle, так что администраторам Windows предстояло жаркое лето. «Изменить такие вещи, как номер порта или текст рассылаемых сообщений, не представляет труда. Я уверен, что это приведет к выбросу новых вариантов Bagle, — как было в феврале и марте», — говорит Гиппонен.

Ричард Штернс, вице-президент по безопасности секьюрити-группы ISSA UK, тоже считал исходный код опасным, но отмечал, что он может содержать подсказки, которые помогут правоохранительным органам выследить автора. В исходном коде содержатся его комментарии, которые могут сузить круг подозреваемых. «Если дать десятку программистов одни и те же спецификации, они напишут десять разных программ. Коды будут подобны, но у каждого программиста есть свои особенности — такие, как имена переменных, методы кодирования, способ комментирования кода. Из этого складывается индивидуальный почерк».

С другой стороны, возможно, что таким способом автор надеялся замести следы. Если исходный код будет присутствовать на множестве компьютеров, то в случае ареста автора код, найденный в его компьютере, перестанет служить уликой против него. Не исключено, что решение о распространении исходного кода было вызвано пятничным объявлением о том, что правительства Великобритании, США и Австралии заключили соглашение о совместной борьбе с распространителями спама.

В январе, через несколько дней после того, как Microsoft и SCO Group назначили приз в $500 тыс. за поимку автора MyDoom, начал распространяться исходный код этого вируса. «Возможно, в данном случае применяется аналогичная тактика. В пятницу наличие в компьютере оригинального исходного кода Bagle было веской уликой против его автора. Сегодня это уже не так», — говорит Гиппонен.