Автор: Артур Скальский © http://www.lenta.ru/ СТРАНА, МИР 1886 20.05.2000, 18:22 241

Новая версия "вируса любви"

В четверг в Интернете начала распространяться новая версия печально известного "вируса любви". Данный штамм более опасен: он наносит больше вреда компьютерам и лучше маскируется в процессе распространения.

Новый вирус NewLove-A распространяется так же, как и ILOVEYOU - в виде вложения в электронные письма. Однако, как передает Associated Press, теперь вместо одной и той же банальной строки "I love you" в заголовке письма каждый раз появляется новая строка, состоящая из "FW:" и случайно выбранного названия файла-вложения из предыдущих писем, полученных пользователем зараженного компьютера. Сам вирус, вложенный в зараженное письмо, также получает имя реального вложения из предыдущей почты пользователя.

Таким образом, письмо с вирусом выглядит как повторная посылка реального письма, которое пользователь уже получал ранее. Единственное отличие - вложенный файл-вирус имеет расширение .Vbs (программа на Visual Basic). Однако и эту "улику" вирус может маскировать: он добавляет к названию файла ложное расширение (Doc, Xls, Mdb, Bmp, Mp3, Txt, Jpg, Gif, Mov, Url, Htm или Txt). Получившийся файл выглядит, например, так: "CWGCXE.Mp3.Vbs". В зависимости от настроек системы настоящее расширение вложенного файла (.Vbs) может быть не показано.

Кроме того, как сообщает Лаборатория Касперского, червь использует полиморфик-алгоритм, меняющий тело программы при каждом заражении - червь дописывает в свой текст случайные строки-комментарии. Таким образом количество строк и, соответственно, размер червя растет от "поколения к поколению", например: 110Kb, 248Kb, 403Kb, 585Kb, 805Kb, 1040Kb и т.д. При этом "чистый" код червя занимает около 5Kb.

Если пользователь все-таки открыл вложение, вирус рассылает свои копии по всем адресам, найденным в адресной книжке почтовой программы MS Outlook на зараженной машине. На самой же машине вирус просто портит большинство файлов на жестком диске - после чего необходимо снова инсталлировать всю операционную систему.

По словам представителя антивирусной компании Trend Micro Inc, уже в четверг от вируса пострадали несколько крупных компаний: в одной из них оказались заражены все ее 5000 компьютеров.

Напомним, что компания Microsoft обещала на следующей неделе выпустить "заплатку", которая позволяет запретить пересылку исполняемых файлов через MS Outlook и таким образом предотвратить распространение некоторых вирусов.

Кроме того, лаборатория Касперского выпустила и бесплатно распространяет антивирус AVP Script Checker, который, по утверждению авторов, защищает не только от червя ILOVEYOU, но и от его мутаций, так как использует уникальную технологию перехвата всех скриптов, посланных на исполнение.

Автор: Артур Скальский © http://www.lenta.ru/ СТРАНА, МИР 1886 20.05.2000, 18:22 241

НАПИСАТЬ ГЛАВРЕДУ:

Телеграм: @babr24_link_bot
Эл.почта: newsbabr@gmail.com

ЗАКАЗАТЬ РАССЛЕДОВАНИЕ:

эл.почта: bratska.net.net@gmail.com

КОНТАКТЫ

Бурятия и Монголия: Станислав Цырь
Телеграм: @bur24_link_bot
эл.почта: bur.babr@gmail.com

Иркутск: Анастасия Суворова
Телеграм: @irk24_link_bot
эл.почта: irkbabr24@gmail.com

Красноярск: Ирина Манская
Телеграм: @kras24_link_bot
эл.почта: krasyar.babr@gmail.com

Новосибирск: Алина Обская
Телеграм: @nsk24_link_bot
эл.почта: nsk.babr@gmail.com

Томск: Николай Ушайкин
Телеграм: @tomsk24_link_bot
эл.почта: tomsk.babr@gmail.com

Прислать свою новость

ЗАКАЗАТЬ РАЗМЕЩЕНИЕ:

Рекламная группа "Экватор"
Телеграм: @babrobot_bot
эл.почта: eqquatoria@gmail.com

СТРАТЕГИЧЕСКОЕ СОТРУДНИЧЕСТВО:

эл.почта: babrmarket@gmail.com

Подробнее о размещении

Отказ от ответственности

Правила перепечаток

Соглашение о франчайзинге

Что такое Бабр24

Вакансии

Статистика сайта

Архив

Календарь

Зеркала сайта