Автор: Артур Скальский © Lenta.Ru ИНТЕРНЕТ, МИР 👁 2399 19.05.2003, 19:46 👍 157

Новый почтовый червь прикрывается именем Microsoft

По состоянию на 19 мая в Интернете зарегистрировано большое количество случаев обнаружения нового сетевого червя Palyh, сооообщает "Лаборатория Касперского".

Указанный вирус маскируется под сообщения от службы технической поддержки Microsoft и распространяется в электронных письмах и ресурсах локальных сетей.

Palyh доставляется на целевой компьютер в виде файла, вложенного в письмо электронной почты или записанного в систему через локальную сеть. При запуске файла-носителя червь активизируется, после чего заражает компьютер и начинает процедуру распространения.

При установке Palyh копирует себя под именем MSCCN32.EXE в каталог Windows и регистрируется в ключе автозапуска системного реестра. Таким образом, червь обеспечивает свою загрузку в память компьютера при старте операционной системы. Из-за ошибки автора вредоносной программы в некоторых случаях Palyh копирует себя в другие каталоги, и в этих случаях функция автозапуска не срабатывает.

Для рассылки по электронной почте Palyh сканирует файлы с расширениями TXT, EML, HTML, HTM, DBX, WAB и выделяет из них строки, похожие на электронные адреса. Затем червь в обход установленной почтовой программы подключается к используемому SMTP-серверу и рассылает через него на найденные адреса свои копии.

В зараженных Palyh письмах всегда указывается фальсифицированный адрес отправителя (support@microsoft.com). При этом темы, тексты и имена вложенных файлов по названиям отличаются. Следует отметить, что все файлы имеют расширение PIF (например, PASSWORD.PIF), хотя на самом деле являются обычными EXE-файлами. В данном случае Palyh использует ложное представление пользователей о безопасности PIF-файлов и недостаток Windows, связанный с обработкой файлов не по расширению, а по внутреннему формату.

Для распространения по локальной сети червь сканирует другие сетевые компьютеры и, если находит на них каталоги автозапуска Windows, записывает туда свою копию.

Несмотря на то, что Palyh нельзя назвать опасным вирусом, у него есть ряд особенностей, представляющих собой потенциальную угрозу для владельцев зараженных компьютеров. Червь имеет функцию загрузки дополнительных компонентов с удаленных web-серверов. Благодаря этому, он в состоянии незаметно устанавливать свои более "свежие" версии или внедрять в систему программы-шпионы.

Автор Palyh встроил в программу временной триггер: если системная дата зараженного компьютера превосходит 31 мая, то червь автоматически отключает все свои функции за исключением загрузки дополнительных файлов. Эта особенность практически обрекает Palyh - web-серверы, откуда он скачивает свои обновления, в ближайшее время будут закрыты.

Автор: Артур Скальский © Lenta.Ru ИНТЕРНЕТ, МИР 👁 2399 19.05.2003, 19:46 👍 157
URL: https://babr24.com/?ADE=7461 Bytes: 2661 / 2661 Версия для печати

Связаться с редакцией Бабра:
newsbabr@gmail.com

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