Trend Micro: червь DOWNAD/Conficker активизируется 1 апреля

Впервые червь Conficker/Kido/DownadUp (по классификации Trend Micro - WORM_DOWNAD.A) был обнаружен в ноябре 2008 года, а новые модификации (классифицированные как WORM_DOWNAD.AD и WORM_DOWNAD.KK) - в начале 2009 г. Червь DOWNAD использует уязвимость в операционной системе Windows, исправленную корпорацией Microsoft (MS08-067) в октябре.

Модификация DOWNAD.AD получила возможность распространяться через сетевые диски и съемные накопители (например, диски USB) с помощью функции автозапуска Windows.

DOWNAD.KK останавливает службы защиты, блокирует доступ с зараженных компьютеров к сайтам разработчиков систем безопасности, а затем загружает троянский конь. Помимо этого, он устанавливает связь с другими зараженными компьютерами через механизмы одноранговой связи и содержит алгоритм обновления зараженных компьютеров.

Для чего предназначен червь?

Судя по всему, задача червя заключается в создании широкомасштабной сети зараженных компьютеров (ботнета) для того, чтобы его разработчики могли рассылать спам, красть личные данные (идентификаторы пользователей, пароли, номера кредитных карт и т.п.) и перенаправлять пользователей на вредоносные сайты с целью фишинга и загрузки других вредоносных программ.

Что произойдет 1 апреля?

Первого апреля 2009 года новейшая модификация червя (WORM_DOWNAD.KK) начнет изменять способ связи с другими зараженными узлами ботнета (настольными компьютерами и серверами), а также попытается связаться с максимальным числом компьютеров в попытках заразить их. На данный момент нет признаков того, что червь предпримет что-либо еще, кроме изменения способа связи.

Как узнать, заражен ли мой компьютер?

Проверьте компьютер с помощью своего продукта Trend Micro или системы HouseCall. Если выяснится, что ваш компьютер заражен, удалите червь согласно инструкциям, приведенным ниже:

Как защитить мой компьютер от заражения?

Немедленно установите исправления для MS08067 и других уязвимостей - сразу же после их выпуска. Включите режим автоматической установки исправлений Microsoft и других разработчиков на своем компьютере.

Убедитесь в том, что ваша антивирусная программа не устарела.

Отключите функцию автозапуска для дисков, чтобы воспрепятствовать заражению с накопителей USB.

Пользуйтесь безопасными паролями из букв, цифр и прочих символов и регулярно изменяйте их.

Соблюдайте осторожность при поиске информации о DOWNAD и Conficker в Интернете. Уже известны поддельные антивирусные программы, разработчики которых пытаются воспользоваться данной ситуацией. Эти программы сообщат, что ваш компьютер заражен, и предложат заплатить за загрузку программы удаления червя, которая в действительности скорее всего окажется очередным вирусом.

Новейшая модификация: WORM_DOWNAD.KK

Этот червь представляет собой пример угрозы нового поколения, при разработке которой мошенники воспользовались различными механизмами заражения компьютеров и распространения вредоносных программ. Инфраструктура Trend Micro Smart Protection Network нейтрализует угрозы до того, как они получают возможность проникнуть в вашу сеть, а наши взаимосвязанные облачные системы оценки репутации файлов, сообщений электронной почты и сайтов позволяют оперативно анализировать и блокировать новые угрозы сразу же после их возникновения. Сегодня системой Smart Protection Network пользуются многие домашние пользователи и предприятия самого разного размера. Дополнительные сведения.