Семейство червей “Code Red”

Автор: Новиков Игнат 141351

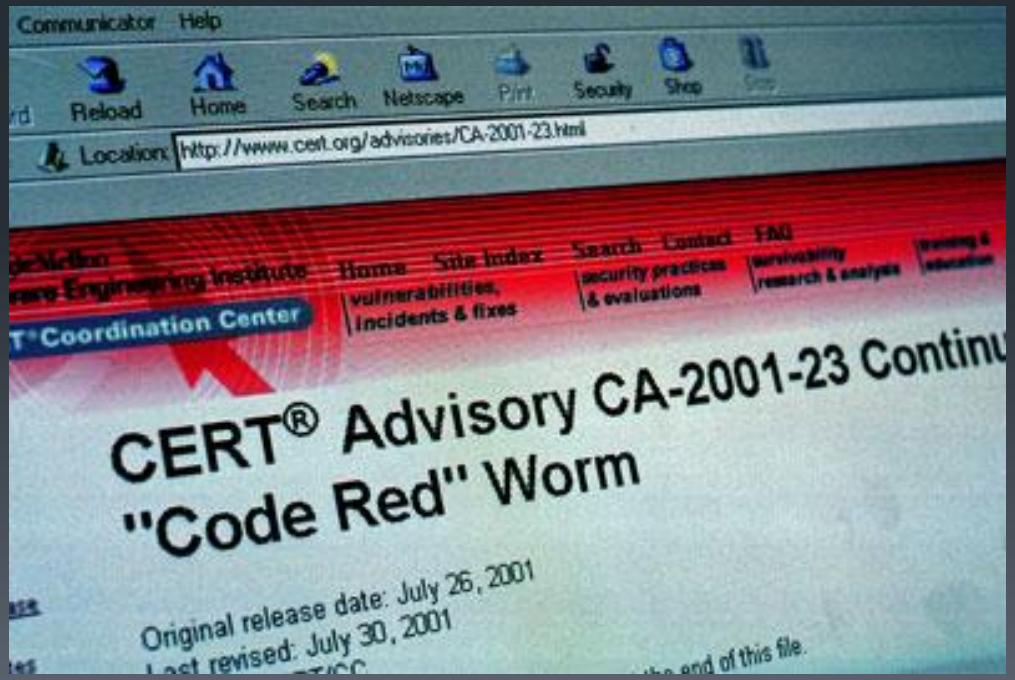
В настоящее время, использование злонамеренного кода типа вирусов, "червей" и "троянов", является одним из наиболее распространенных видов атак в Интернет. Все современные IT организации, использующие любые виды подключений к Интернет, должны быть готовы к отражению такого вида нападений.

Червь:

или саморазмножающийся вирус это определенный вид злонамеренного кода, он отличается от остальных видов вирусов способностью самопроизвольного размножения без вмешательства пользователя. Принимая во внимание тот факт, что традиционные вирусы требуют определенного взаимодействия с пользователем, будь-то запуск программы или загрузка какого-нибудь компонента с Web сайта, в то же время "черви" способны к размножению вообще без каких-либо взаимодействий с пользователем или системой.

Настоящее признание черви получили после атаки вируса Code Red в июле 2001 года.

CodeRed (19 июля, 2001) — представитель нового типа зловредных кодов, способных активно распространяться и работать на зараженных компьютерах без использования файлов. В процессе работы такие программы существуют исключительно в системной памяти, а при передаче на другие компьютеры — в виде специальных пакетов данных.

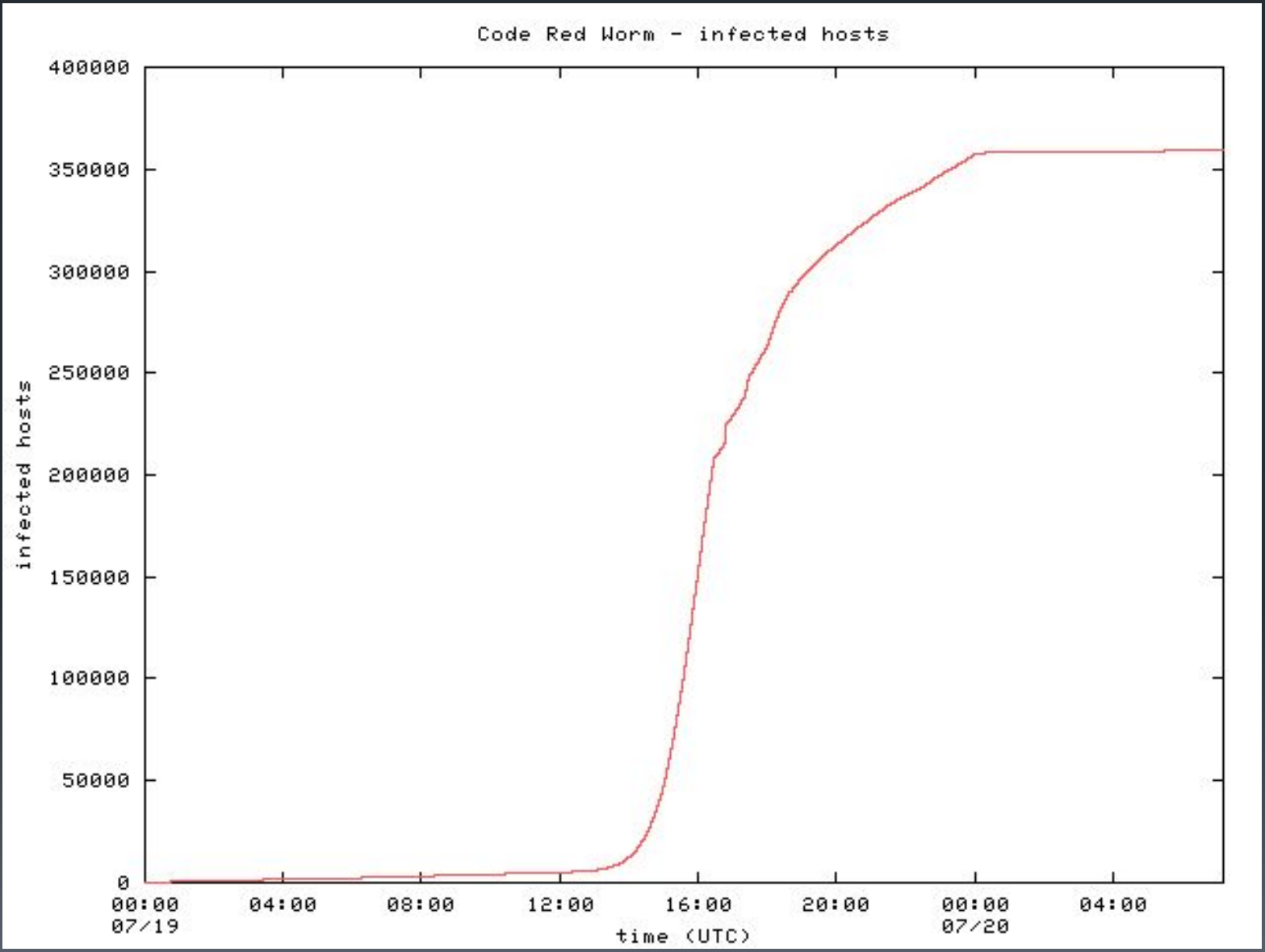


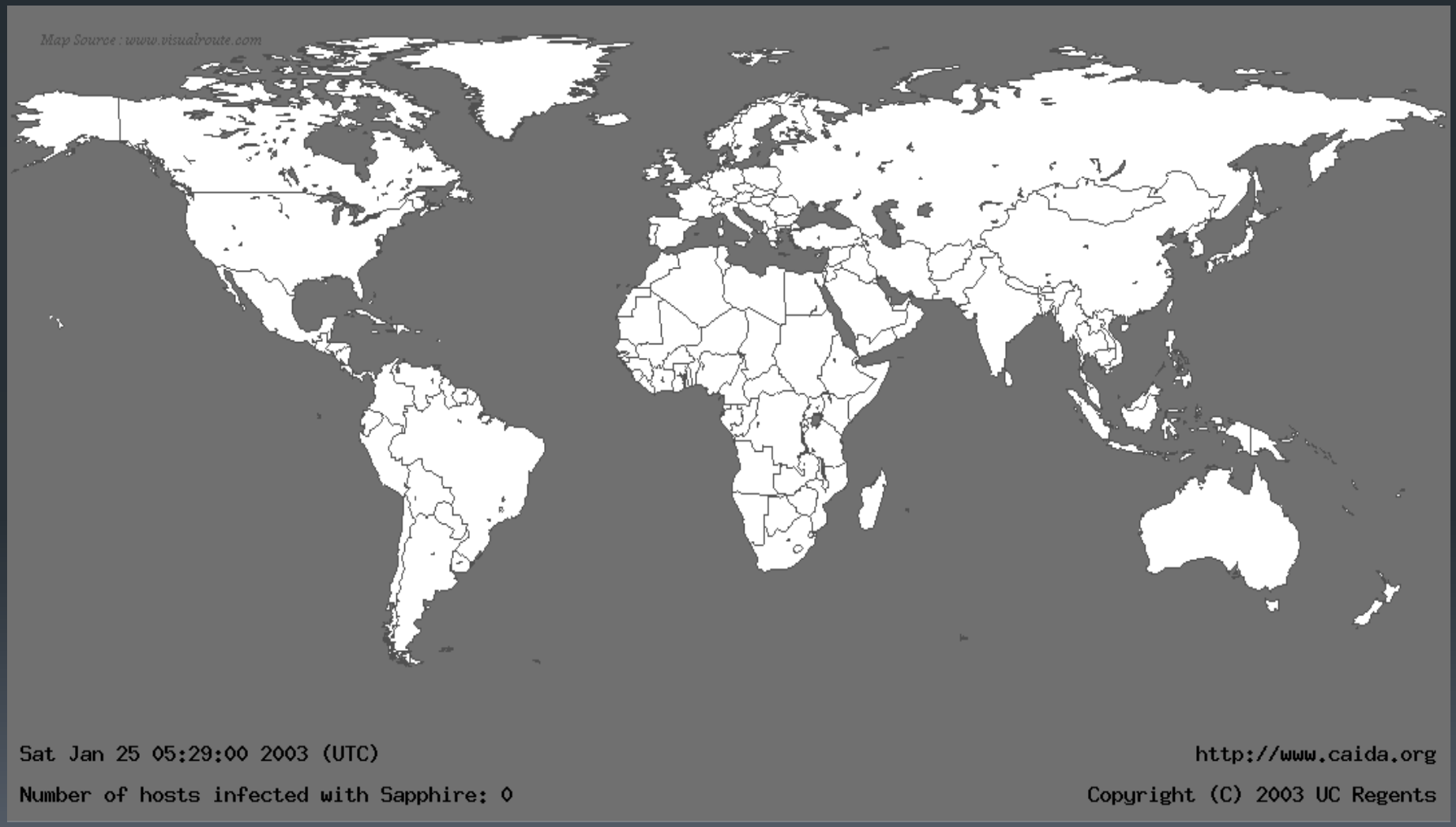
eEye Digital Security®

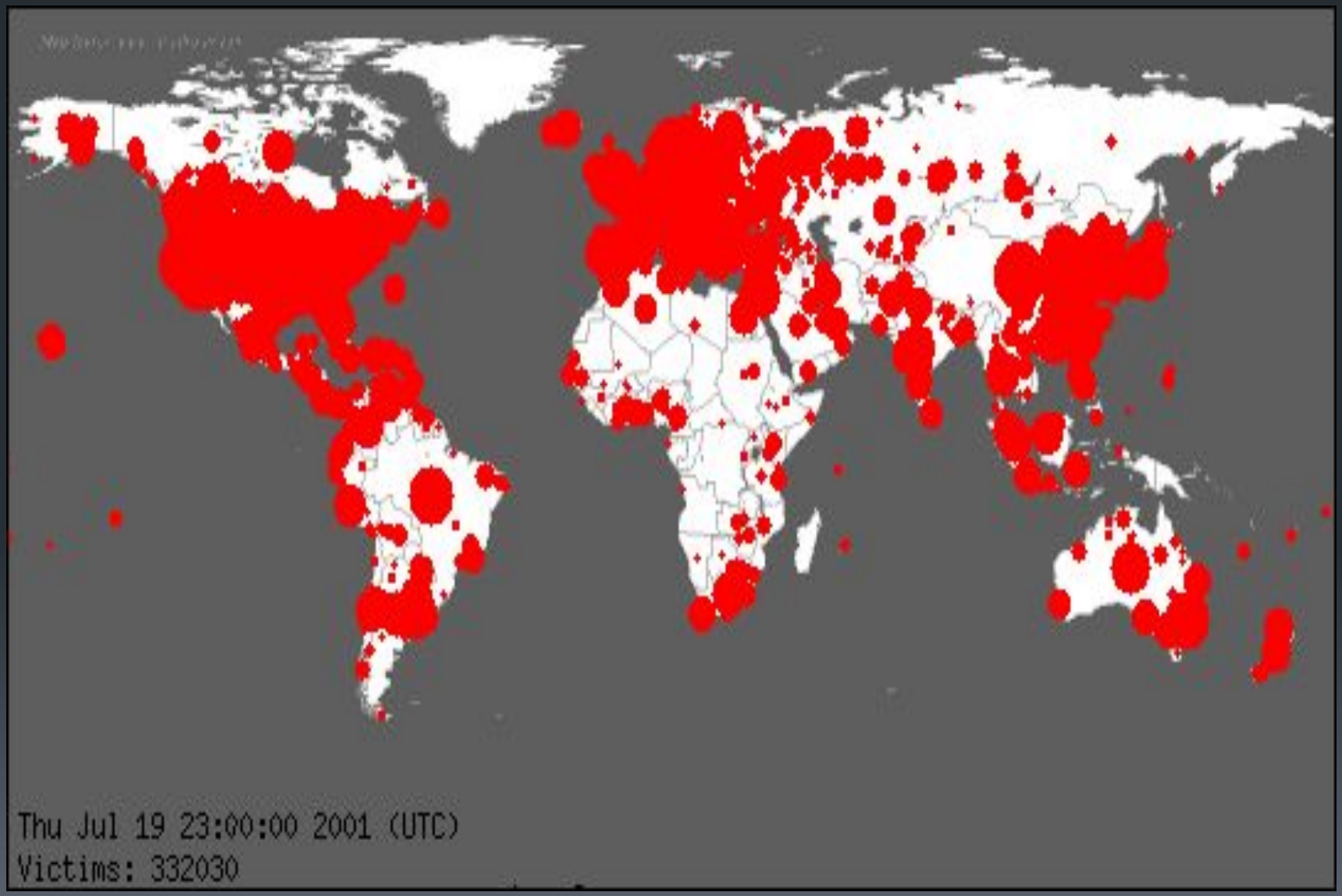
- Самое подробное и оперативное описание и анализ червя были сделаны программистами группы eEye Digital Security. Они также дали вирусу название — намек на вид напитка Mountain Dew и фразу-предупреждение в вирусе Hacked By Chinese! («Взломано китайцами!») — намек на коммунистический Китай, хотя в действительности вирус, скорее всего, был написан этническими китайцами на Филиппинах. Этой фразой червь заменял содержимое веб-сайтов на зараженном сервере.

Червь использовал уязвимость в утилите индексирования, поставлявшейся с веб-сервером Microsoft IIS, позволяющую выполнение случайного кода с привилегиями под которыми, как правило, работает IIS сервер (обычно LocalSystem). Эта уязвимость была описана вендором — Microsoft — на их сайте MS01-033 (англ.). Кроме того, за месяц до эпидемии была опубликована соответствующая заплатка.

Немного статистики…




Map Source : www.visualroute.com
Sat Jan 25 05:29:00 2003 (UTC)
Number of hosts infected with Sapphire: 0
http://www.caida.org
Copyright (C) 2003 UC Regents


Thu Jul 19 23:00:00 2001 (UTC)
Victims: 332030

Принцип работы и главная цель

- Вирусы подобные Code Red атакуют порты узлов широко использующих открытые http службы.
- Проявления, изначально заложенные в Code Red, заключались в использовании всех зараженных им компьютеров для организации DOS-атаки против веб-сайта Whitehouse.gov (веб-сайта Белого дома).

- Так же у червя Code Red была и вторая версия. Вирусы Code Red первой и второй версий использовали подпрограмму случайной выборки адресов, хотя в первой версии был недостаток, заключающийся в том, что при каждой активизации вируса он пытался атаковать один и тот же список IP адресов. Во второй версии "червя" этот недостаток был устранен и, следовательно, он мог поражать большее количество компьютеров, заражая хосты, пропущенные ранее первой версией. Скорость заражения второй версии червя была 11 пакетов в секунду. Вскоре, 4, августа 2001 года, начал распространяться новый червь Code Red II, код которого, несмотря на схожее название, был создан заново.

Используемые источники

- 1) http://www.dgl.ru/articles/camye-opasnye-virusy-za-vsu-istoriu-sushhestvovaniya-komputerov_4566.html
- 2) https://ru.wikipedia.org/wiki/Code_Red
- 3) http://www.securitylab.ru/analytics/216325.php

Спасибо за внимание!!