

ЦТП "Доктор Веб"

Обзор вирусной обстановки за май 2009 г. от компании «Доктор Веб»

Компания «Доктор Веб» представляет обзор вирусной активности в мае 2009 г. В прошедшем месяце продолжилось распространение программ-вымогателей. Киберпреступники оттачивают методы социальной инженерии, создают более изощренные инструменты, облегчающие их мошенническую деятельность. Появляются все новые руткиты. Спамеры используют новые способы прохождения спам-фильтров. Среди мусорной почты, как и ранее, увеличивается доля писем, рекламирующих сами спам-рассылки.

Выпуск новых версий сканера с графическим интерфейсом

В мае 2009 г. компания «Доктор Веб» выпустила несколько новых версий сканера Dr.Web с графическим интерфейсом для Windows. Это было сделано для оперативного противодействия новым вирусным угрозам: модификации буткита BackDoor.Maosboot и троянцу Trojan.AuxSpy.

Trojan.AuxSpy блокирует запуск и мешает работе некоторых утилит, способных помочь его обезвредить (например, редактора реестра). Несмотря на то, что троянец не работает в режиме ядра системы, он прописывается в нестандартную область системного реестра, а также может восстанавливаться из памяти.

Появление подобных вредоносных программ лишней раз свидетельствует о том, что пользователю в настоящее время необходимо обновлять не только базы вирусных описаний используемого антивируса, но и все его компоненты.

Уязвимость в браузере Safari

В середине мая стало известно об уязвимости в браузере Apple Safari версии 3.2.3, а точнее — в одной из его библиотек, в компоненте libxml. Уязвимость позволяет выполнить произвольный код при посещении специальной web-страницы, подготовленной злоумышленниками, а также может быть использована для инсталляции в систему злонамеренного кода. Данная уязвимость присутствует в браузерах Safari для платформ Mac OS X и MS Windows. В последнее время наблюдается все большая активность киберпреступников по отношению к системам с Mac OS X.

Спам

В мае 2009 г. общее количество спам-сообщений осталось на уровне прошлого месяца. Можно отметить продолжающееся увеличение количества сообщений, направленных на привлечение новых клиентов спамеров. Среди аргументов перечисляются: существенный результат, который может приносить реклама с помощью спама, законность данного способа рекламы, использование услуг спамеров крупными компаниями и пр. Конечно, данные заявления лишь отчасти соответствуют действительности либо являются целиком вымыслом спамеров.

Постепенно увеличивается количество спам-сообщений с предложениями быстро заработать в Интернете или поучаствовать в очередной финансовой пирамиде.

Фишинг-рассылки

Несмотря на их низкую эффективность, продолжают классические фишинг-рассылки. Жертвами мошенников становятся клиенты все новых онлайн-систем, связанных с денежными операциями. Так, в мае прошли фишинг-рассылки, нацеленные на пользователей системы Comerica Business Connect банка Comerica Bank (США).

Вредоносные файлы, обнаруженные в мае в почтовом трафике (01.05.2009 00:00 – 01.06.2009 00:00)

1. Win32.HLLM.Netsky.3532814813173(41,31%)
 2. Win32.HLLM.Beagle3612033(10,07%)
 3. Win32.HLLM.MyDoom.338083554352(9,91%)
 4. Win32.HLLM.Netsky.286722425299(6,76%)
 5. Win32.HLLM.MyDoom.441568617(4,37%)
 6. Win32.HLLM.Netsky.based1403727(3,91%)
 7. Win32.HLLM.Perf1056208(2,95%)
 8. Win32.HLLM.MyDoom.based820918(2,29%)
 9. Trojan.MulDrop.19648661200(1,84%)
 10. Win32.HLLM.Beagle.32768627811(1,75%)
 11. Trojan.MulDrop.13408626816(1,75%)
 12. Win32.HLLM.Netsky578837(1,61%)
 13. Win32.HLLM.MyDoom.49554956(1,55%)
 14. Exploit.IFrame.43481410(1,34%)
 15. Trojan.PWS.Panda.114391321(1,09%)
 16. Win32.HLLM.Beagle.27136378735(1,06%)
 17. Win32.HLLM.Netsky.28008362897(1,01%)
 18. Win32.HLLM.Graz277064(0,77%)
 19. Win32.HLLM.Beagle.pswzip260037(0,73%)
 20. Exploit.IframeB0175968(0,49%)
- Всего проверено: 163 867 066 697
Инфицировано: 35 861 521 (0,0218%)

Вредоносные файлы, обнаруженные в мае на компьютерах пользователей (01.05.2009 00:00 – 01.06.2009 00:00)

1. Win32.HLLW.Shadow.based2347116(18,99%)
 2. Win32.HLLW.Gavir.ini723353(5,85%)
 - 3 Trojan.AuxSpy.13506981(4,10%)
 4. VBS.Generic.548285643(2,31%)
 5. Win32.HLLW.Autoruner.2536274582(2,22%)
 6. Win32.HLLW.Autoruner.5555270656(2,19%)
 7. DDoS.Kardraw248823(2,01%)
 8. Trojan.Download.35128243625(1,97%)
 9. Trojan.DownLoader.42350225703(1,83%)
 10. Win32.Sector.17219578(1,78%)
 11. Win32.Alman210942(1,71%)
 12. Trojan.Starter.544206115(1,67%)
 13. Win32.Virut.14198389(1,61%)
 14. Win32.HLLM.Netsky.35328196459(1,59%)
 15. Win32.HLLM.Beagle155071(1,25%)
 16. Trojan.AuxSpy.15143727(1,16%)
 17. Win32.HLLW.Autoruner.274136360(1,10%)
 18. Trojan.Botnetlog.9131285(1,06%)
 19. Trojan.AuxSpy.7122566(0,99%)
 20. Trojan.Download.36194121743(0,99%)
- Всего проверено: 99 061 889 355
Инфицировано: 12 358 946 (0,0125%)

Контактная информация

Сергей Кравченко, PR-консультант ЦТП «Доктор Веб»

E-mail: sergey.kravchenko@drweb.com.ua