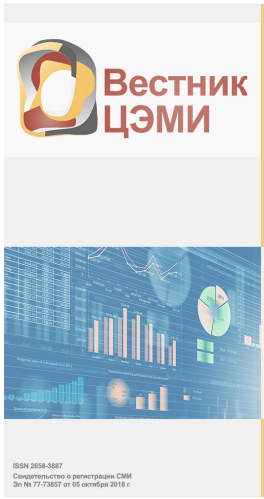

Вестник ЦЭМИ РАН. 2018-2019

ISSN 2658-3887

URL - http://cemi.jes.su

Все права защищены

Выпуск 3 Том . 2018

Неравномерность запросов пользователей к АВ-серверу

Терентьев А. М.
Центральный экономико-математический институт РАН
Российская Федерация, Москва

Аннотация

Исследованы запросы пользовательских ПК на антивирусные обновления. Написана оригинальная программа, задействующая логи программы Apache. Вывод программы оформлен в виде HTML-таблицы, содержащей список IP-адресов и число их обращений за нужные дни. Таким образом, Антивирусный сервер получил новую функцию Статистики. Функция позволяет получить сводку за один или несколько дней подряд о числе пользователей и числе их обновлений в эти дни. Эта функция доступна для любого пользователя Антивирусного web-сайта.

Ключевые слова: антивирус, сервер, Apache, HTML, DrWeb

Дата публикации: 12.01.2019

Ссылка для цитирования:

Терентьев А. М. Неравномерность запросов пользователей к АВ-серверу // Вестник ЦЭМИ РАН. 2018. Выпуск 3 [Электронный ресурс]. Доступ для зарегистрированных пользователей. URL: http://cemi.jes.su/s111111110000008-1-1 (дата обращения: 14.01.2019). DOI: 10.33276/S0000008-1-1

1 Снабжение пользователей института антивирусными средствами

предусматривает использование антивирусного сервера (АВ-сервера) как промежуточных мест хранения антивирусных обновлений пакетов Doctor Web (32-битного и 64-битного) [3] [8] [4] [5] [6], используемых в ЦЭМИ РАН с 2003 г.

2 В настоящее время число активных пользователей обоих вариантов DrWeb несколько превышает 100; несколькими годами ранее наблюдалось до 210 пользователей. Тому есть несколько причин. Во-первых, из 350 сотрудников института далеко не все имеют приписанные к ним ПК. Во-вторых, централизованное антивирусное обслуживание исполняется только для ПК, закупленных ЦЭМИ РАН, но не личных ПК пользователей (например, ноутбуков). В-третьих, уже несколько лет недостаток финансирования потребовал исключения антивирусного обслуживания серверов и сокращение числа лицензий на рабочие ПК. В-четвёртых, ряд пользователей сознательно не используют DrWeb, предпочитая альтернативные антивирусные средства. Наконец, в-пятых, текущие версии пакетов DrWeb 6.0 Security Space пригодны для обслуживания Windows' 2000 / XP / Me / Vista / 7 / 8 / 9, но уже для Windows'10 непригодны (хотя несколько пользователей Windows'10 у Антивирусной службы имеются).

3 Автором уже давно замечено [7], что в различные дни недели число пользователей, получающих антивирусные обновления, меняется. Представляет определённый интерес, насколько велико это число в различные дни недели в настоящее время, когда основной состав пользователей DrWeb в институте давно определён.

4 Подсчёт актуальных пользователей института ведётся с февраля 2006 г, на АВ-сайте в разделе «Статистика» [2] формируются соответствующие таблицы. Однако, этой информации оказалось недостаточно, иногда интересуют более детальные сведения. Для этого в разделе «Статистика» создано специальное приложение на основе оригинальной программы автора. Оно позволяет за выбранные сутки (одни или несколько подряд) подсчитать число обращений к АВ-серверу за антивирусными обновлениями. Подсчёт ведётся на основе обращений к файлу **drweb32.lst** в различных каталогах антивирусных обновлений, независимо от успешности завершения обновлений.

5 На рис. 1 приведена форма обращения к этим статистическим данным. Затребованы сведения за неделю, начиная с понедельника 14 мая 2018 года. Результаты расчёта приведены на рис. 2.

6

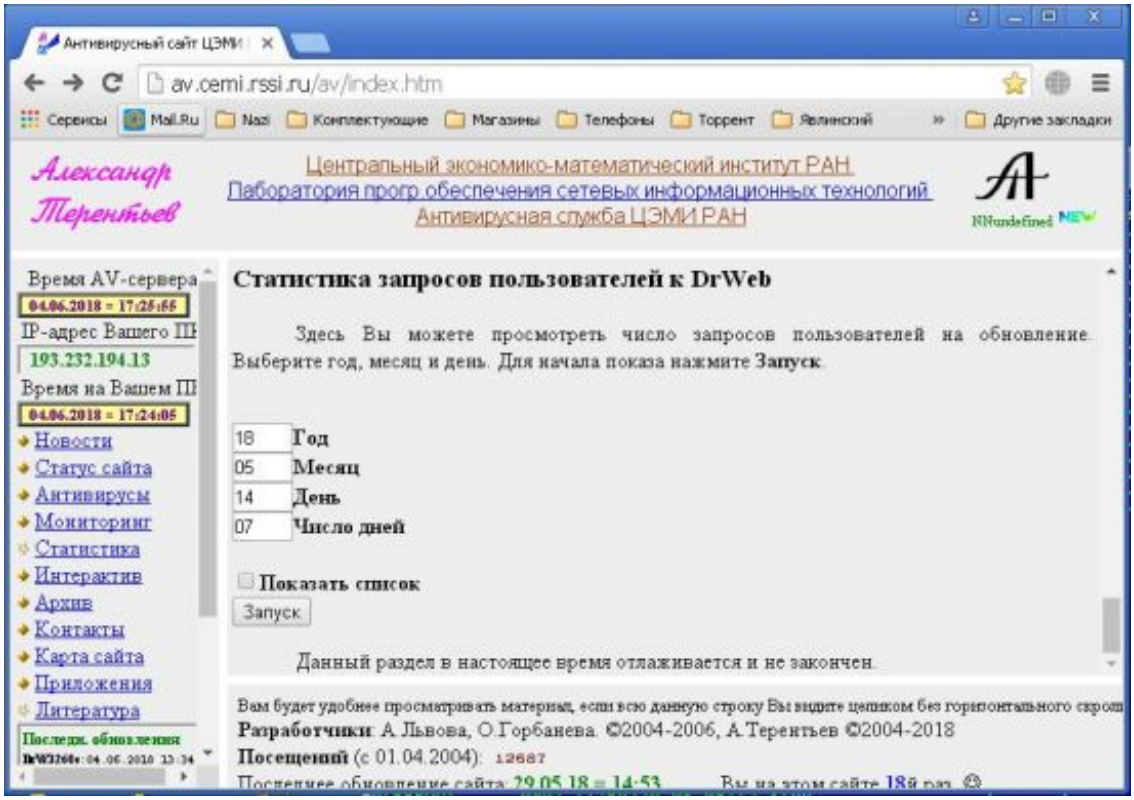

Рис. 1. Форма запроса на число обращений пользователей

7

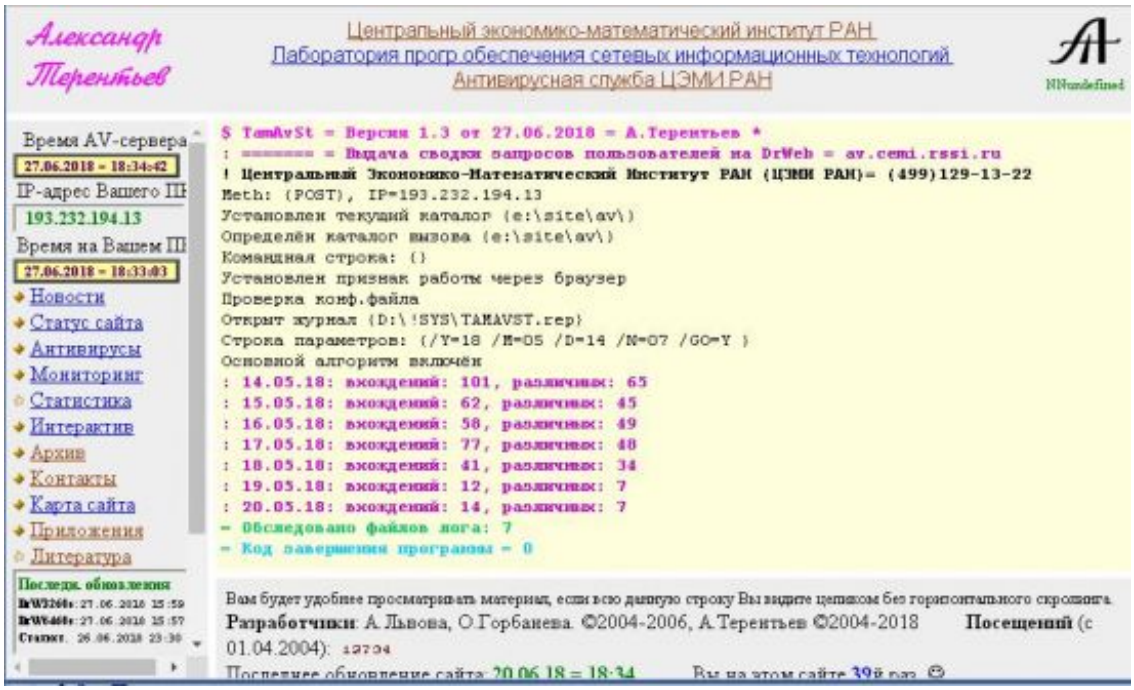

Рис. 2. Результат запроса по форме рис. 1

8 Следует пояснить, что один и тот же ПК может в течение рабочих суток несколько раз обращаться к Антивирусному серверу (хотя бы потому, что на большинстве ПК обращение за антивирусными обновлениями настроены на исполнение при включении компьютера, а ряд пользователей включает ПК несколько раз за день). Поэтому, в частности, с 65 различных ПК в понедельник 14.05.18, как явствует из рис. 2, было выполнено всего 101 обращение.

9 Представляет интерес распределение числа включавших компьютер по дням недели. Как видно из рис. 2, и это типовой результат, максимальное число достигается за понедельник, 2/3 от него в четверг с уменьшением в остальные дни недели.

10 Программа позволяет показывать и детальные сведения по обращениям. Например, автора заинтересовало необычно большое число обращений в воскресенье, 20 мая. Для этого был сделан отдельный запрос, причем проставлена галочка в поле «Показать список». Результат показан на рис. 3.

11

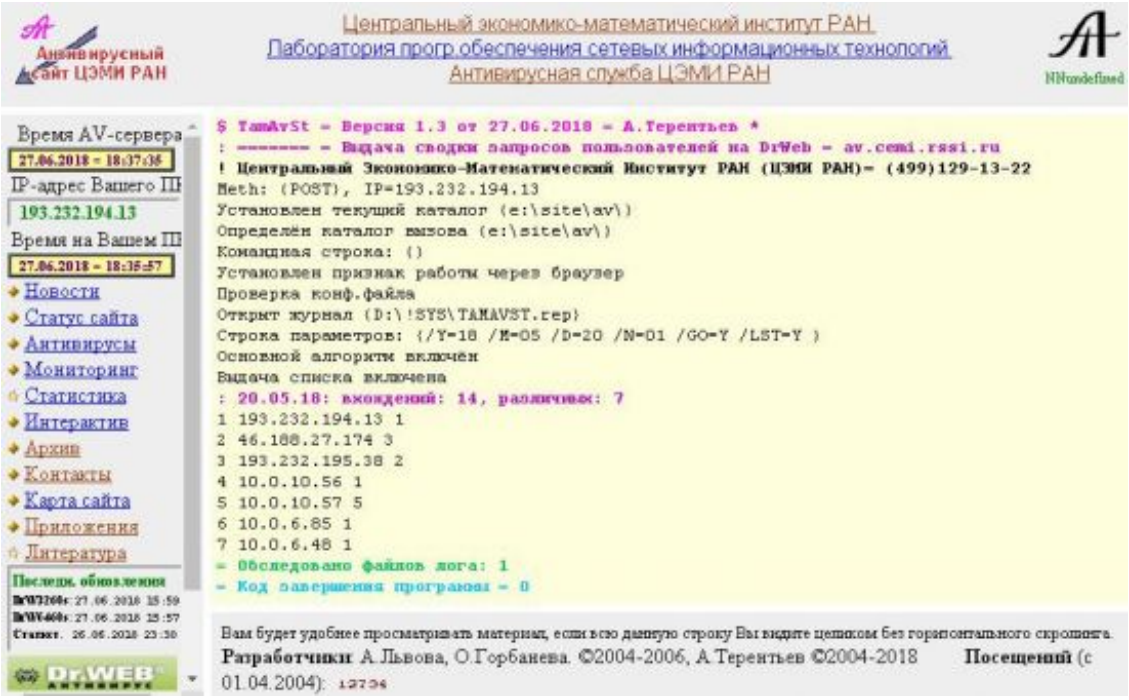

Рис. 3. Детальные сведения за воскресенье, 20 мая 2018 г

12 Результаты показывают, что в воскресенье 20 мая были запросы на антивирусные обновления от 7 компьютеров:

13 – 1 обращение от адреса 193.232.194.13 (это постоянно включённый рабочий ПК Антивирусной службы);

14 – 3 обращения от внешних пользователей (2 рабочих ПК автора на дому, один из которых включался 2 раза);

15 – 2 обращения от рабочего ПК Сетевого центра (к.921), вероятно, от двух дежуривших в разное время пользователей;

16 – по 1 обращению от пользователей ПК 10.0.10.56, 10.0.6.85 и 10.0.6.48;

17 – 5 обращений от ПК 10.0.10.57.

18 Последний случай – особый. Адрес 10.0.10.57 закреплен за ПК администратора лаборатории Б.Е.Бродского, нерегулярно и в необычные дни бывающего на рабочем месте. По этим причинам Антивирусной службе до сих

пор не удалось исправить ошибку при установке антивирусного пакета на этом ПК, вследствие чего активным осталось задание в Планировщике заданий на антивирусное обновление каждые полчаса. За 2 часа работы поэтомубыло исполнено 5 обращений, считая начальное.

19 Запросы означенных типов допускаются для задействования любым пользователем Антивирусного сайта. Как можно видеть из рис. 2 и 3, в протоколе остаётся IP-адрес, с которого был сделан запрос. Протоколы всех запросов сохраняются на АВ-сервере.

20 Программа **tamavst.exe** написана на языке PowerBASIC Console Compiler 5.05 [1] и достаточно тривиальна. Она запускается при заполнении формы, осуществляя HTML-вывод в формы указанных видов. Программа, как и большинство программ-утилит автора, имеет конфигурационный файл, позволяющий легко настроить её работу на особенности вычислительной среды эксплуатанта. Программа самодокументирована: её запуск как консольного приложения (непосредственно с сервера) без параметров вызывает выдачу нескольких страниц технического встроенного Help'а.

21 В настоящее время активными являются две области антивирусных обновлений – "***DrWeb для рабочих станций x86 Security Space***" и "***DrWeb для рабочих станций x64 Security Space***" (исключительно для Windows'7+x64). В различное время существования АВ-сервера с 2003 г было задействовано до 7 различных областей. Разработанная программа позволяет извлекать данные по сумме всех областей за любой из дней работы сервера с 2004 г.

22 Задействование указанной технологии позволяет получить качественно новый вид информации об активности пользователей антивирусных средств АВ-сервера. В отдельных случаях, подобно показанному выше на рис. 3, можно выявить ошибки в настройке ПК.

Uneven user requests to the Anti-Virus server

A. Terentjev
CEMI RAS
Russian Federation, ,

Abstract

The requests of the user's PC for anti-virus updates were investigated. The original program that uses Apache logs is written. The output of the program is designed as an HTML-table containing a list of IP-addresses and the number of their calls for the desired days. So, the anti-virus server received a new Statistics function. This function allows you to get a summary for one or several days in a row about the number of users and the number of their updates on these days. This feature is available to any user of the anti-Virus web site.

Keywords: antivirus, server, Apache, HTML. DrWeb

Date of publication: 12.01.2019

Citation link:

Terentjev A. Uneven user requests to the Anti-Virus server // Vestnik CEMI RAS. 2018. Issue 3 [Electronic resource]. Access for registered users. URL: http://cemi.jes.su/s111111110000008-1-1 (circulation date: 14.01.2019). DOI: 10.33276/S0000008-1-1

Код пользователя: 7792; Дата выгрузки: 14.01.2019; URL - http://cemi.jes.su/s111111110000008-1-1 Все права защищены.