Худолій Іван Іванович
викладач інформаційних систем Аграрного коледжу управління і права ПДАА,
викладач вищої кваліфікаційної категорії, викладач – методист,
hudoliy_ivan@mail.ru

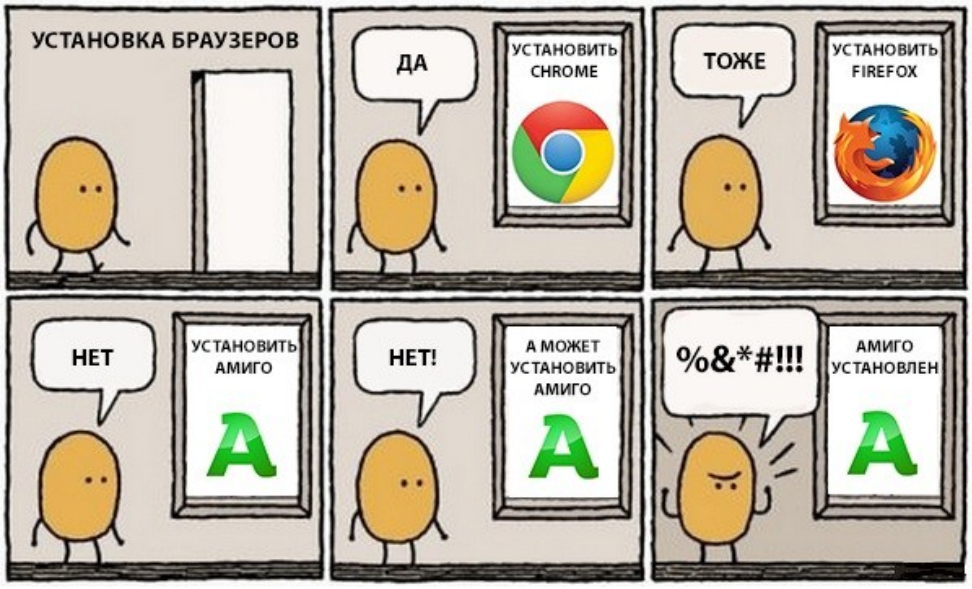
БРАУЗЕР АБО ВІРУС? ЗАХИСТ ВІД ВІРУСНОГО БРАУЗЕРА «АМІГО»

"Користувач не знає, чого хоче, поки йому це попередньо не встановити без його бажання й замовлення"

Генрі Форд

Ідея написання цієї статті виникла після того як кількість персональних комп'ютерів моїх студентів – активних користувачів інтернетом, що потрібно «лікувати» від нав'язливого маркетингу офіційних постачальників інтернет-послуг почала прямувати до 100%.

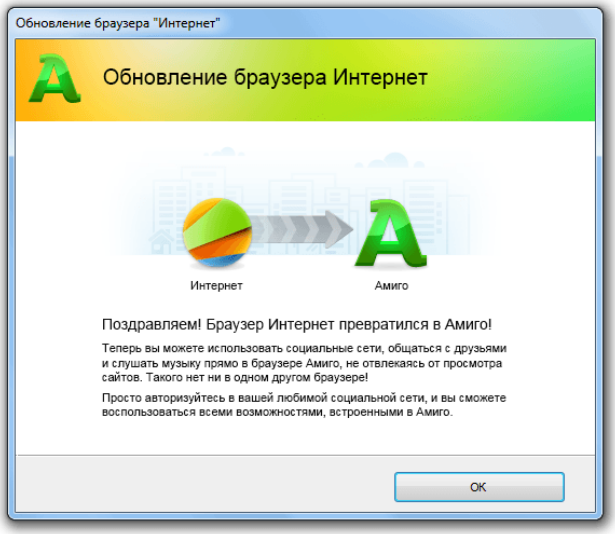
Сталося так, що програми від mail.ru вміють досить агресивно рекламувати одна одну за допомогою не зовсім коректних спливаючих вікон. Але прогрес не стоїть на місці, а розробники браузера **Аміго** дуже багато сил вклали в інноваційність свого продукту. Наприклад, зуміли винайти приголомшливу фішку - браузер навчився завантажуватися і встановлюватися на комп'ютер у фоні, нічого не питаючи у користувача. Навіщо його турбувати, так?



Про групу компаній Mail.ru вже давно гуляють невтішні відгуки та думки про їх агресивному і нечесному маркетингу не тільки по відношенню до конкурентів, але і, в першу чергу, по відношенню до самих користувачів.

Виною всьому не тільки триклятий браузер Аміго але й Guard і Downloader від Mail.ru. Вся справа в тому, що ці нібито "корисні" (за заявами розробників) програмки, поводяться ніяк інакше, як шкідливі об'єкти. Чому так? Поясню. Наприклад, вирішили ви собі встановити мейл.ру агент, гру, що закачано з інтернету, безкоштовну програму, закачати програму з торента або з іншого файлообмінника. Завантажили, інсталюєте, і тут відбувається найцікавіше - крім самої програми, на ваш улюблений комп'ютер встановлюється ще купа усіляких приблуд: супутник, тулбар, Гуард, аміго, пошук в інтернеті і т.п. За заявами представників мейл.ру, якщо ви знімете "галочку" з цих програм при установці основної програми, то вони і не будуть встановлені. Але, на ділі це далеко не завжди так. Свідченням тому служить безліч гнівних реплік, відгуків та оглядів з цього приводу.

Але головний "козир" mail.ru - це GuardMailRu (нібито Захисник). Справедливості заради, варто відзначити, що він, звичайно, захищає від несанкціонованої зміни стартової сторінки браузера, наприклад, або ж від несанкціонованої зміни пошукової машини. Але, в цьому-то і вся заковика. Він, практично без відома користувача, встановлює стартову сторінку MailRu. І ось від її зміни і захищає. Також і з пошуком за замовчуванням. Причому не тільки захищає, але і видаляє всі раніше встановлені модулі від Гугла, Яндекса, Рамблера і т.п.



Здавалося б, та й чорт з ним, корисна ж функція (з одного боку). Але, справа в тому, що при видаленні Guard, він магічним чином повертається знову. І все - ваша стартова сторінка навіки Mail.ru)

Хто хоч трохи знайомий з інформаційною безпекою вже, напевно, побачили шкідливу природу всіх цих дій, характерну для вірусів і троянів. Наприклад:

- ***встановлення без відома користувача;***
- ***зміна налаштувань без відома господаря;***
- ***видалення додатків сторонніх розробників;***
- ***відсутність можливості видалення стандартними засобами операційної системи.***

«Спасибі» за таку турботу, шановні розробники. Не могли б ви наступного разу видалити всі інші браузери? І драйвера оновити? А, можливо, переустановити операційну систему, змінити прізвище господаря комп'ютера, продати його квартиру, одружити і змінити громадянство?

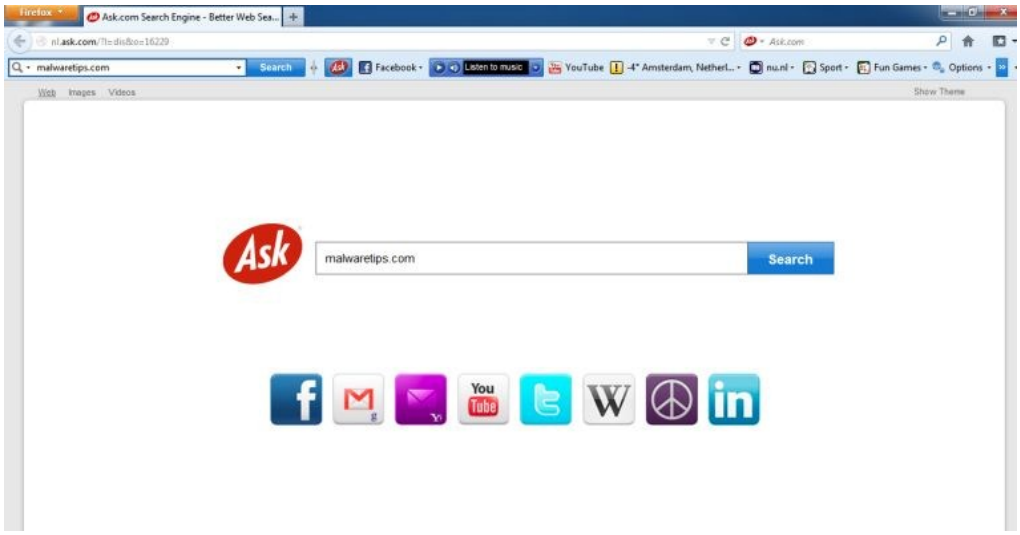
Але це ще не все. Як з'ясувалося, у mail.ru є ще один "додаток" - Downloader (Завантажувач). І ось це вже реальне шахрайство з боку цієї компанії. Пояснюю. Гуляє, наприклад, інтернет-користувач по різних ресурсам у мережі, шукає необхідну інформацію, і тут - бац - вискакує повідомлення, що вам необхідно оновити скайп, оперу, мозіллу, хром, інтернет експлорер, флеш-плеєр і т.п., причому виглядає це все цілком офіційно. АЛЕ! Викачування йде не з офіційного сайту, а з сайтів-партнерів mail.ru, і викачується, звичайно ж, не оновлення, а Браузер Аміго все від тієї ж Mail. ru! Природно зі своїм тулбаром та іншої непотрібної "гидотою", типу спутника@mail.ru.

Чому ж антивіруси не блокують ці продукти? Виявляється, всі ці псевдооновленія підписані справжнім і легітимним цифровим підписом Mail.Ru! Тому антивіруси цілком природно довіряють викачаному і запущеному додатку.

"Не ми перші це почали". Ось так співробітник Mail.ru, що має безпосереднє відношення до розробки downloader`a, відповів на авторитетному інтернет порталі на численні претензії і реальні факти, засновані на аналізі коду та поведінки цього "завантажувач", які дозволяють сміливо заявити: Downloader від Mail.ru - це ні що інше, як троян!

Компанії якось потрібно монетизувати свої проекти. От і вирішили вони піти по шляху "партнерських програм" - пропонують різних ресурсів спосіб заробітку, за допомогою цього самого "завантажувача".

Хоча, справедливості заради варто відзначити, що подібний агресивний маркетинг реально придумали не в mail.ru. У Яндекса, наприклад, теж є свій "Захисник". Різні сервіси типу AOL, Ask.com, ICQ і т.п. також використовують установку своїх тулбарів або програм в сторонньому софті, причому роблять це давно.



Але те, на що пішли в Mail.ru, відкрито обманюючи користувачів помилковими оновленнями сторонніх програм - це, звичайно, нонсенс.

Як же оберегти себе і свій комп’ютер від цих проблем?

Щоб запобігти їх установку є наступні варіанти:

- ✓ Встановити програму Unchecky, яка блокує установку сторонніх програм
- ✓ Заборонити установку прихованих програм за допомогою AppLocker, тільки для Windows 7 Ultimate або Professional
- ✓ Обмежити доступ до облікового запису користувача

- ✓ Блокування установки прихованих програм за допомогою Unchecky

Програма Unchecky дозволяє запобігти установці небажаних програм прибираючи галочки при запуску завантаженого файлу з інтернету. А також попереджає чи є у файлі сторонні програми, які можуть встановитися, без вашої згоди. Установка проста і не викликає у труднощів.

У Windows 7 Ultimate або Professional існує зручна програма AppLocker , яка не дозволяє встановлення програм із заборонного списку.

Завантажте файл настройок Locker до себе на комп'ютер і розпакуйте його в папку. Відкрийте Панель управління - Адміністрування - Служби

Знайдіть службу «Посвідчення додатки» (Удостоверение приложения) Переведіть її в режим автозапуску і запустіть.

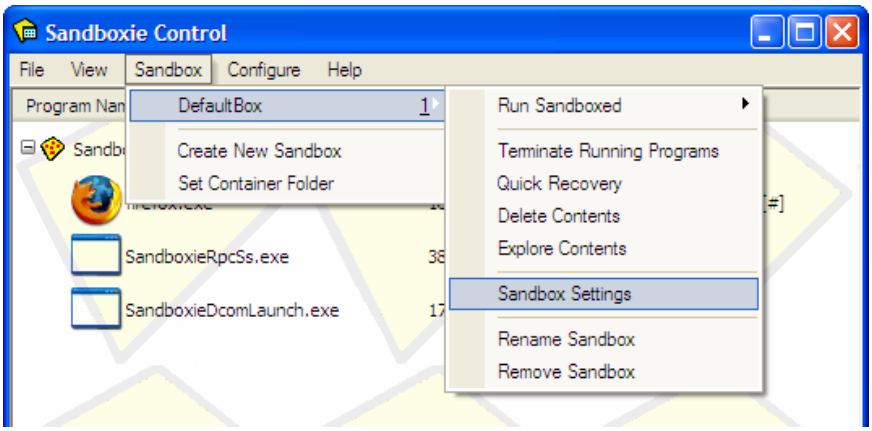
Відкрийте Панель управління - Адміністрування - Локальна політика безпеки. Знайдіть Політика управління додатками. Натисніть правою кнопкою на параметр AppLocker

Натисніть Імпортувати політику.

Знайдіть і відкрийте файл з раніше завантаженого архіву «Locker.xml»

Тепер жодна програма від зазначених видавців не зможе проникнути на цей комп'ютер. Всі вони будуть блоковані ще на стадії установки.

Програма Sandboxie дозволяє запустити веб браузер в захищеній області та відкривати файли без шкоди установки зайвих програм. При установці можна вибрати потрібну мову. Після в самій програмі Sandboxie вже можна створити пісочницю і запустити браузер . Сама програма інтуїтивно з зрозумілим інтерфейсом і труднощів у користувача не повинно виникати.

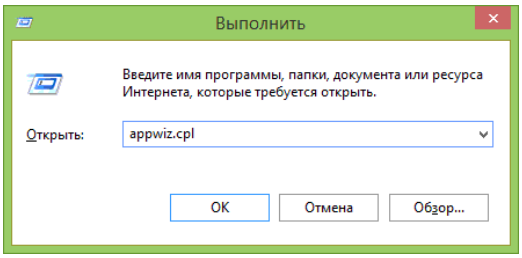


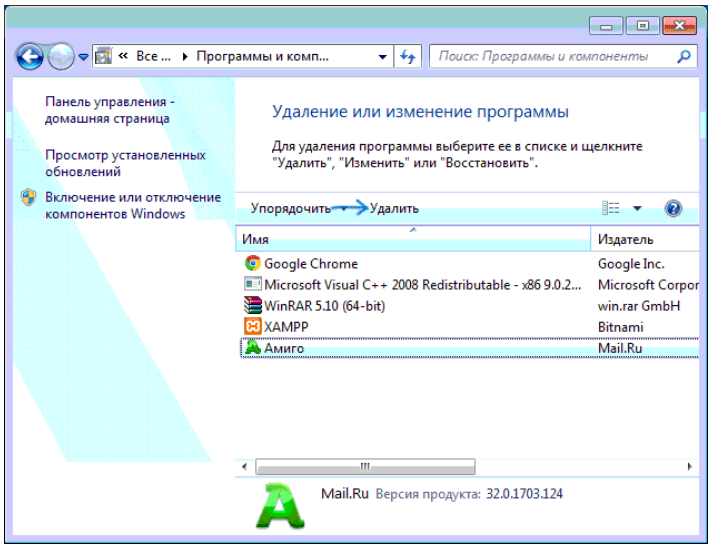
До речі, в деяких хороших антівірусника вже присутня Sandbox , наприклад в Avast Premium або Internet Security с віртуальним кабінетом SaveZone.

Але що робити, якщо Аміго з різноманітними додатками встановлено? Як повністю видалити вірусний браузер з вашого комп'ютера? На перший погляд недосвідченого користувача все просто: знаходимо програмний файл, тиснемо Shift - Del і прощаємося назавжди з набридливим «Другом - Аміго». У таких випадках щастя тривати буде недовго. Після першого ж перезавантаження системи «Аміго», як казковий фенікс, відроджується на колишньому місці. У подібних ситуаціях необхідно видаляти не тільки саму програму, але й вичищати її «коріння» з системи.

Нижче я пропоную покрокове керівництво як видалити «Аміго» з комп'ютера правильно і назавжди.

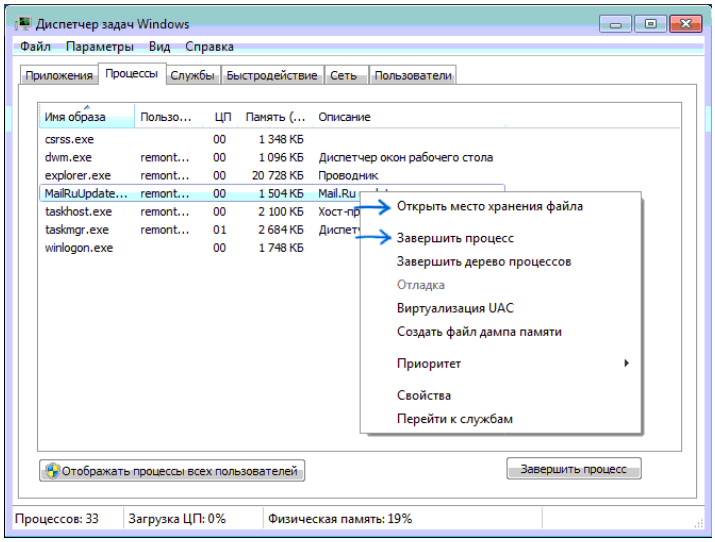
Викликаємо через кнопку Пуск-Панель управління . Шукаємо розділ «Установка та видалення програм» (в деяких версіях Windows він іменується «Програми та засоби»). Для досвідчених користувачів є більш швидкий спосіб зайти в розділ, що цікавить: за допомогою вікна «Виконати», яке відкривається при натисканні комбінації Win + R. У полі введення потрібно вбити команду appwiz.cpl , як показано на малюнку нижче.

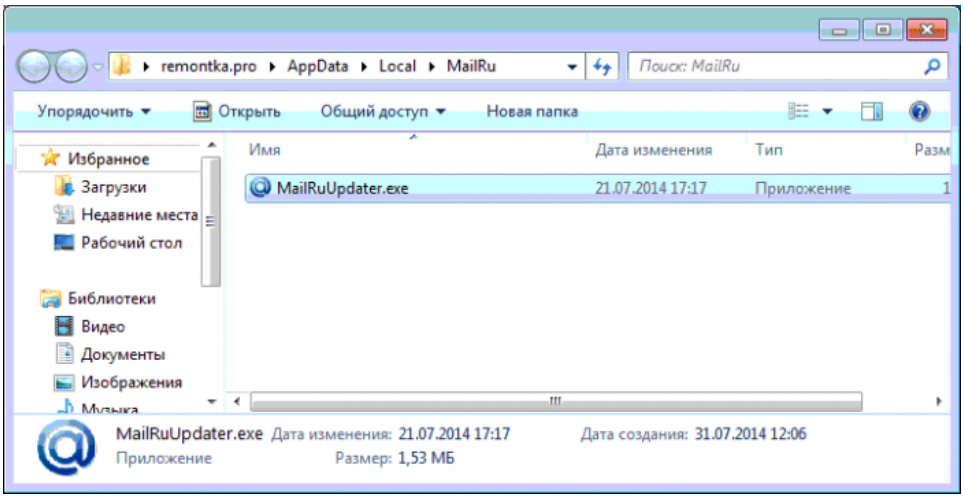




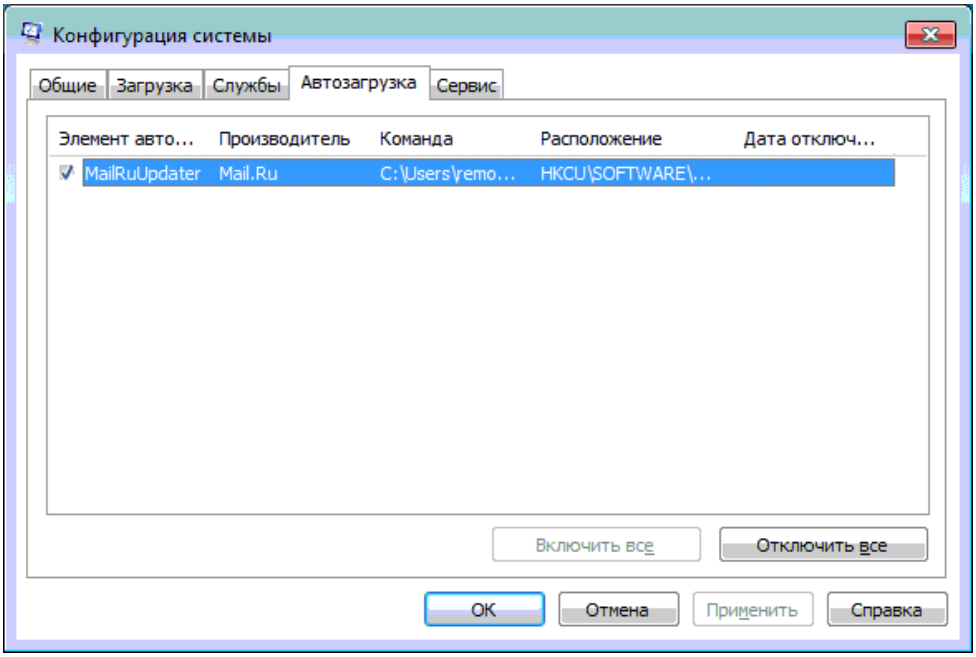
Шукаємо у списку програм браузер «Аміго», клацаємо по ньому правою кнопкою миші і обираємо «Видалити з контекстного меню», після чого запуститься процес видалення. Але це, нажаль, ще не все . Якщо у вас вже був невдалий досвід видалення вірусного браузера, що не приніс результатів, значить десь в системі лежить файл «Mail.ru Updater», який і є винуватцем повторної «мимовільної» установки програми. А це означає, що необхідно позбавитися і від нього.

Натискаємо комбінацію клавіш Ctrl + Alt + Del. У вікні диспетчера задач активуємо вкладку Процеси знаходимо MailRuUpdater.exe. Клацнувши правою кнопкою мишки знаходимо місце зберігання файла і відключаємо сам процес, знищуємо файл у теці.





І нарешті, фінальний крок – потрібно убрати «MailRu Updater» з автозавантаження . Натисніть комбінацію Win + R і введіть msconfig . У вкладці «Автозавантаження» вибираємо шуканий файл і, клацнувши по ньому все тієї ж правою кнопкою миші, викликаємо контекстне меню і прибираємо його з автозавантаження .



Не забудьте, що будь які зміни у роботі системи вимагають перевантаження комп’ютера.

Маю надію, що дана стаття допоможе активним користувачам послугами інтернет позбавиться від нав’язливого вірусного браузера.