УДК 004.056.3

ФЛЕШКАДАҒЫ ВИРУС ЖОҒАЛТҚАН АҚПАРАТТАРДЫ ҚАЛПЫНА КЕЛТІРУ

Ысқақ Н.А.
Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана қаласы

Ғылыми жетекші – Ұзаққызы Нұргүл

Бұл мақалада aadrive32.exe(Backdoor.win32.ruskill) вирусы флешкадағы жоғалтып жіберген файлдарды қалай қалпына келтіруге болатыны жайлы, ол вирустан қалай құтылуға болатындығы жайлы қарастырылған.

aadrive32.exe вирусы. Бұл вирус флешка арқылы таралады. Флешканы компьютерге қоссаңыз болғаны ол келесідей әрекеттерге көшеді:

– Флешкада Recycler (себет іспеттес) папкасын жасайды, сол папкаға кездейсоқ атпен EXE файлын көшіреді.

– Флешканың түп тамырында жатқан барлық файлдардың атрибуттарын жасырын және жүйелікке (скрытыми и системными) ауыстырады.

– Файл аттарымен ярлыктар жасайды (*.lnk), қолданушы бұл ярлыктарды ашқан кезде вирус іске қосылады, керек файл ашылуы мүмкін [1].

Негізі бұл вирусты қазіргі кезде антивирустар тауып залалсыздандыра алады. Егер сізде антивирус болмаған жағдайда вирустан келесі әрекеттерді жасап құтылуға болады:

– Documents and Settings\USERNAME\Application Data каталогынан *.exe және *.tmp файлдарын жою қажет.

– windows\system32 каталогынан 14.exe, 38.exe-ге ұқсас файлдарды жою қажет

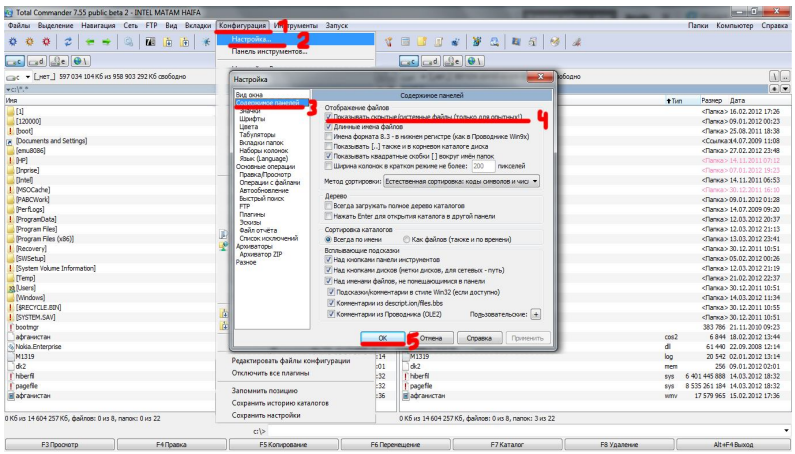
– windows каталогынан aadrive32.exe файлын жою қажет.

– c:\Recycler каталогынан күмәнді файлдарды жоямыз. Егер себетіңізде қажетті файлдар болмаса онда папканы толығымен жойып жіберуге болады [2].

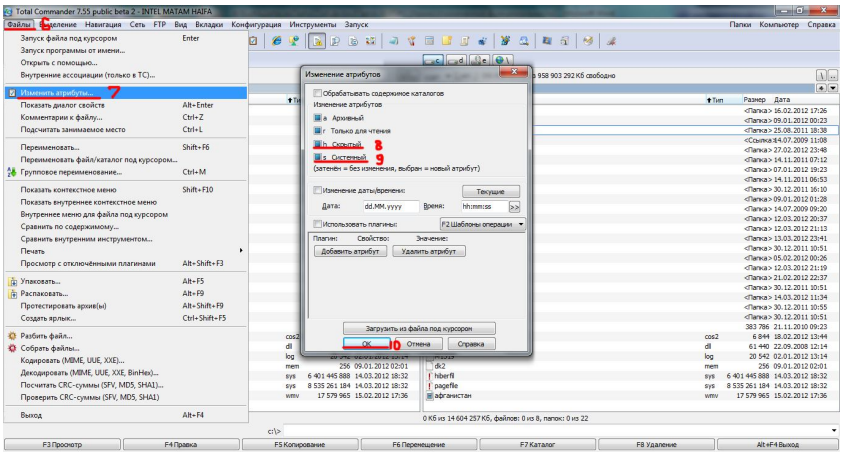
Көптен күткен файлдарды қалпына келтіруге де келіп жеттік. Файлдарды қалпына келтірудің бірнеше жолдары бар:

1. "Total Commander" бағдарламасының көмегімен. Біріншіден бұл бағдарламада жасырын файлдарды көрсету функциясын іске қосуымыз керек (сурет-1). Сонан соң флешканың әйнегіне көшеміз. Бұл жерде барлық файлдарды таңдаймыз (Ctrl-A). Файл атрибуттарын қалпына келіреміз (сурет-2). Бұл бағдарламаны мына сілтеме бойынша жүктеп ала аласыз:

http://nur-kz.ucoz.net/load/total_commander_7_55_rus_plugins/1-1-0-49 [3].



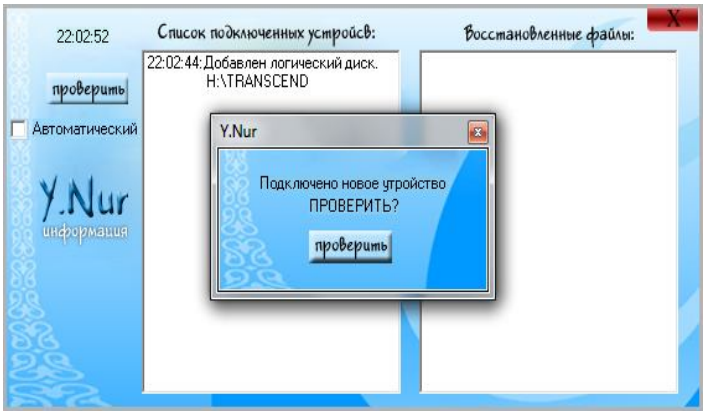
Сурет -1.



Сурет-2.

2. "BAT" файлының көмегімен. Мынандай құрылымды файл көмегімен: **attrib -S -H /D /S** Бұл BAT файлды флешкаға саламыз және сол жерден іске қосамыз. Жасырын тұрған файлдар көрінуі керек.

3. "Восстановление данных на флешке" бағдарламасының көмегімен (сурет-3).



Сурет-3.

Бұл бағдарлама флешкадағы вирус жасаған барлық ярлықтарды өшіріп, файлдардың жасырын және жүйелік атрибуттарын алып тастайды, яғни файлдарды қалпына келтіреді. Жаңа қондырғы қосылған кезде бірден "Жаңа қондарғы қосылды. Тексерейін бе?" деген хабарлама шығады. Егер тексер десеңіз бағдарлама өз ісіне кіріседі. Бұл бағдарламаны мына сілтеме бойынша жүктеп ала аласыз:

http://nur-kz.ucoz.net/load/vosstanovlenie_dannykh_na_fleshke/1-1-0-50 [4].

Қорыта келсек флешкаңыз вирустанып файлдарыңыз жоғалса, форматтауға асықпаңыз. Антивирустар тек вирустан тазалайды, ал жоғарыда көрсетілген бағдарламалар файлдарды қалпына келтіруге арналған.

Әдебиеттер

1. http://jenyay.net/blog/2011/05/24/pro-virus-aadrive32-exe/
2. http://acid.name/?p=555
3. http://nur-kz.ucoz.net/load/total_commander_7_55_rus_plugins/1-1-0-49
4. http://nur-kz.ucoz.net/load/vosstanovlenie_dannykh_na_fleshke/1-1-0-50