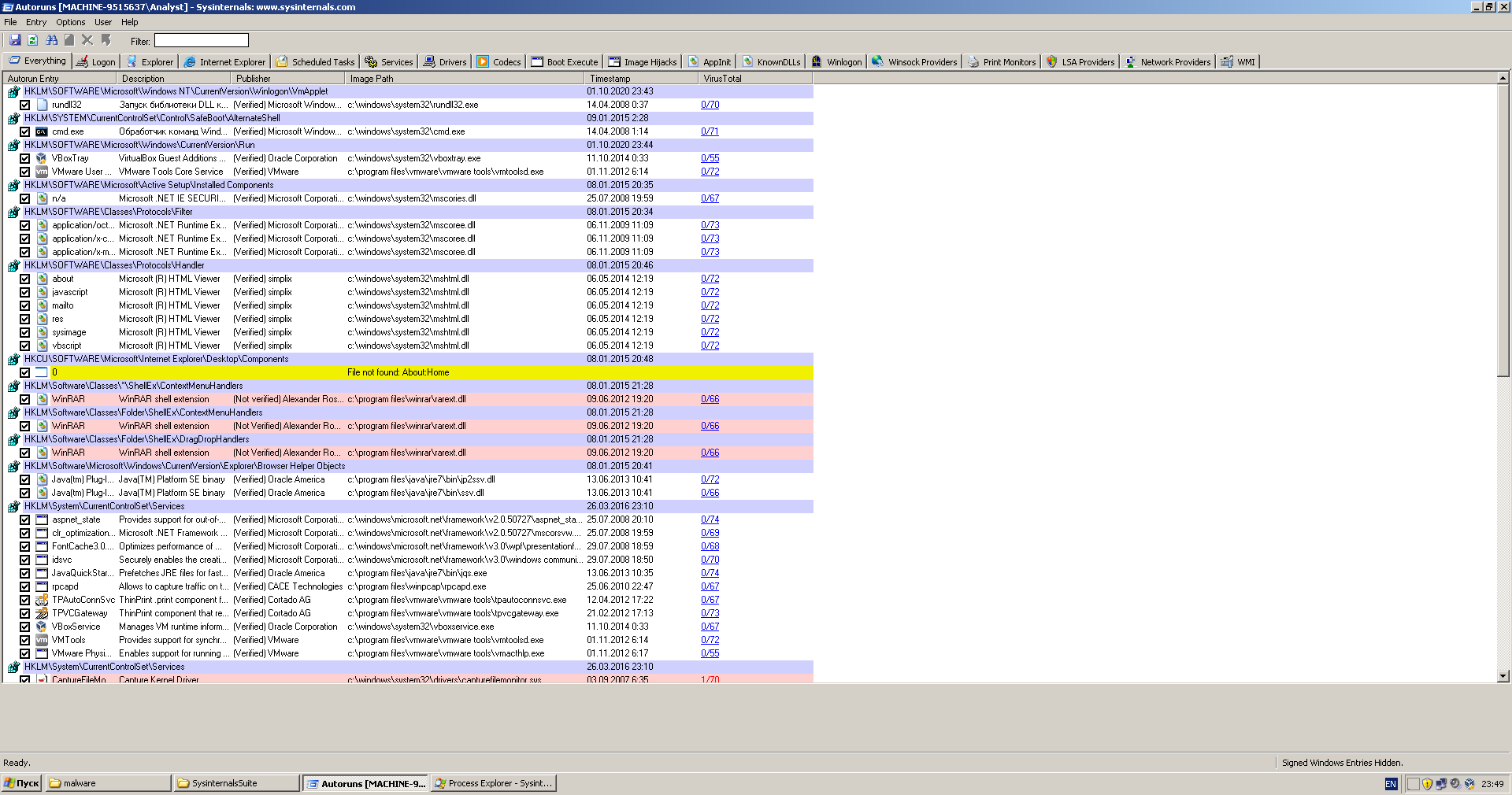
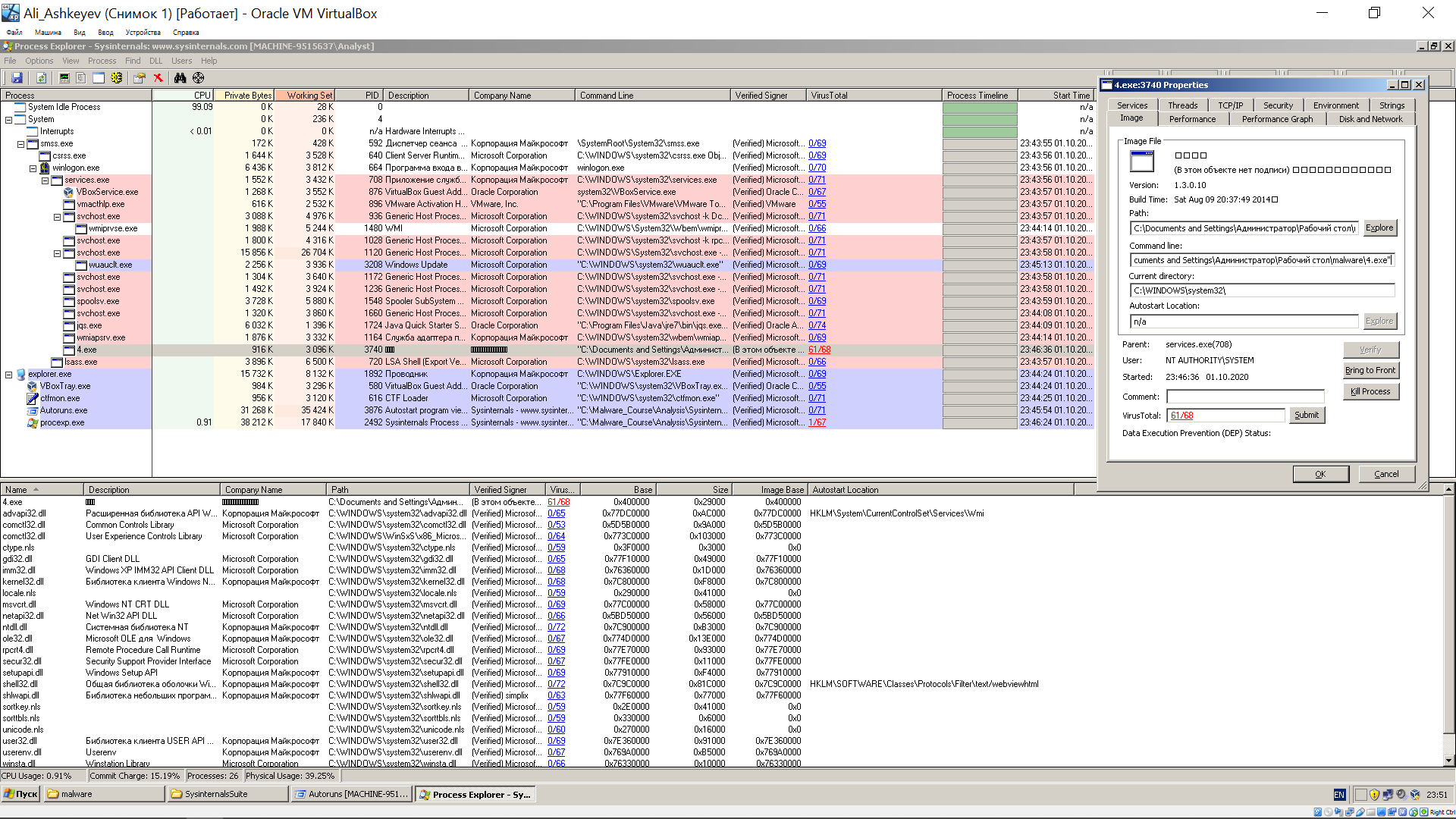
Ashkeyev Ali 18BD11079

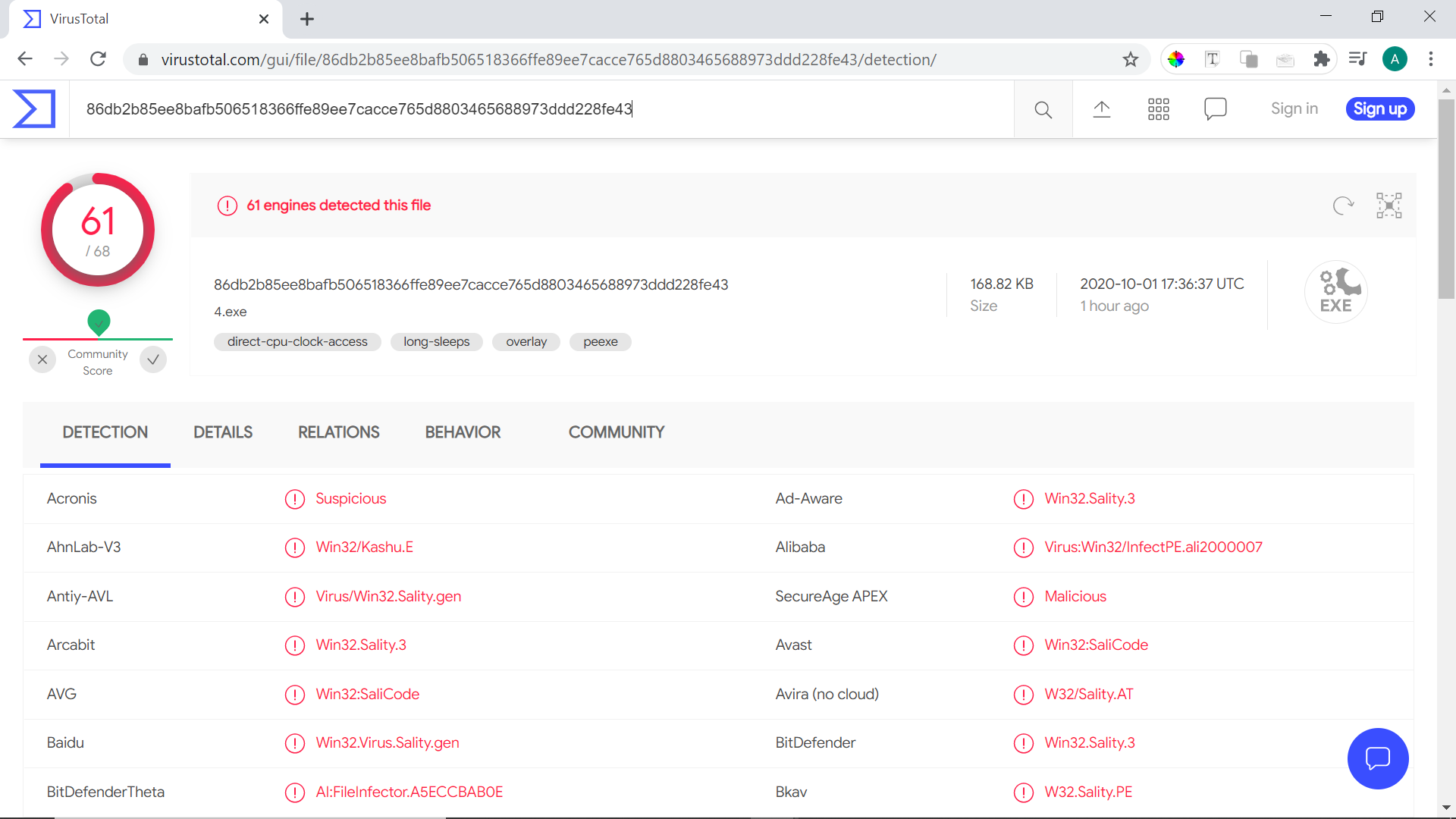
The problem with 4.exe malware is it does not detect in Autorun it means we can not kill the process from autorun. After starting processexplorer it was found that 4.exe located into the service.exe with the same directory.

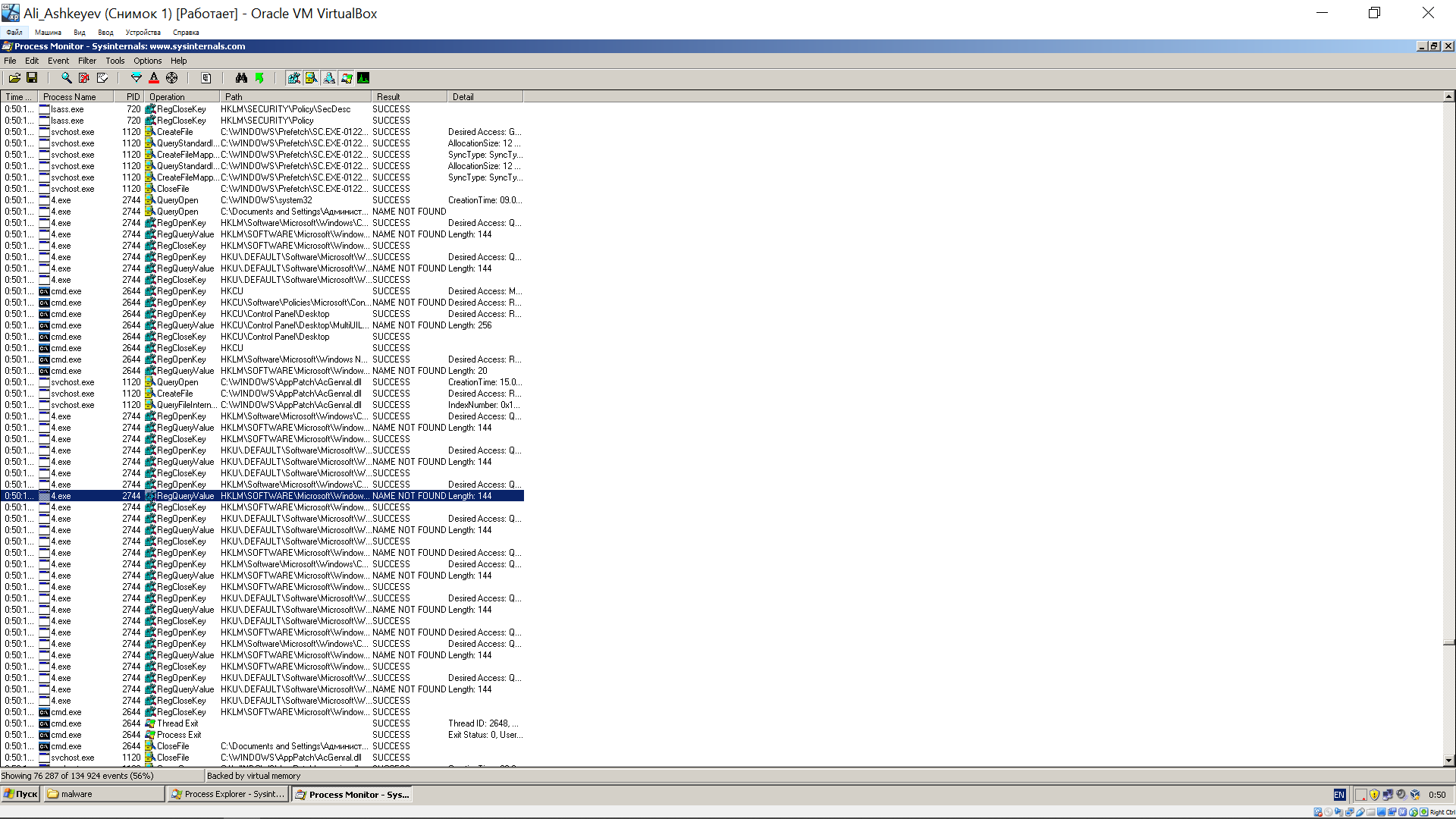


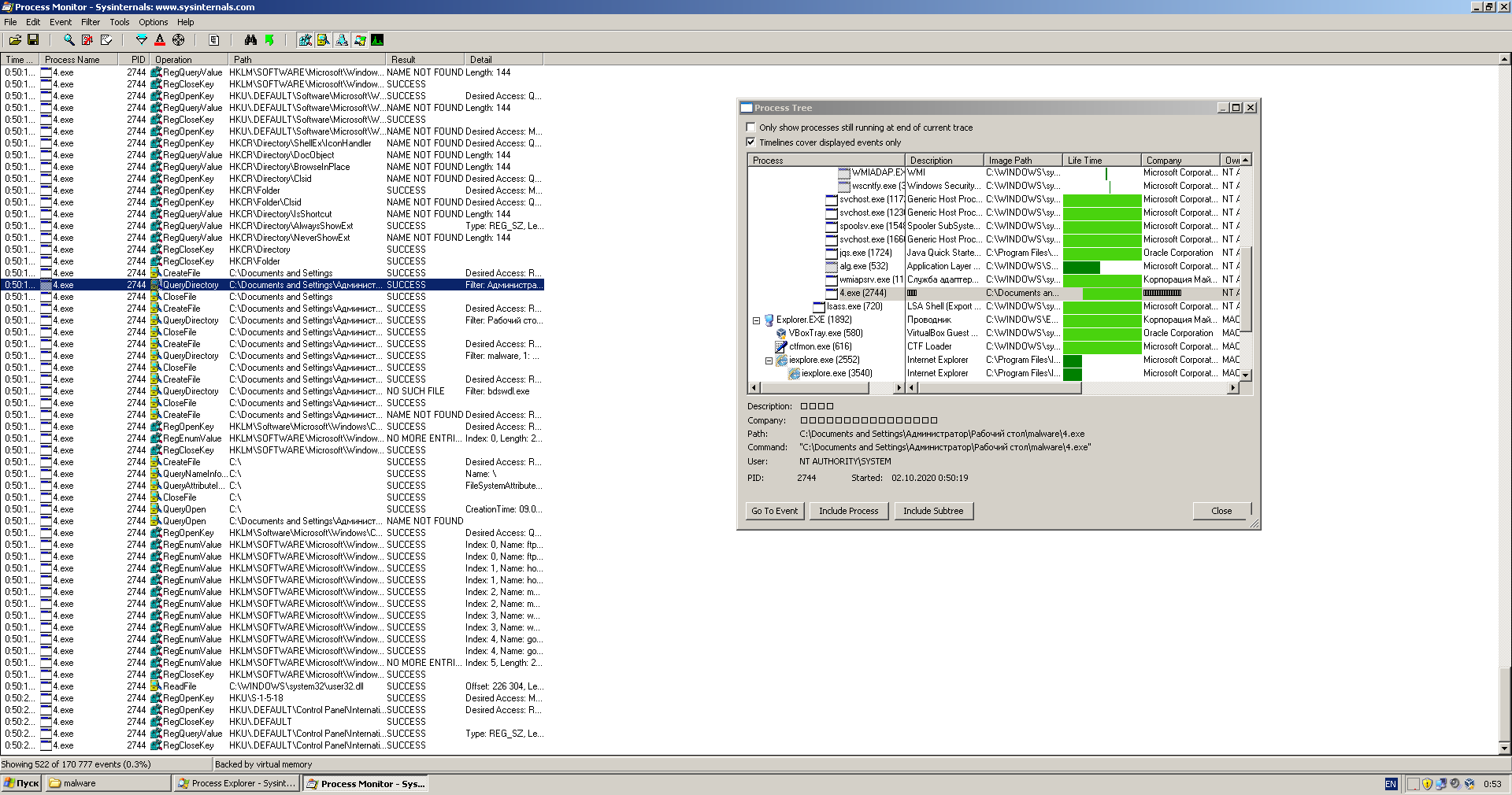
In this screenshot it is shown that 4.exe has not verified certificate, this is the first signal that it is malware, moreover in virus total from 68 antiviruses 61 says that it is malware.



In the website virustotal.com we can find that this virus known as Sality and short description is written, also there are list of antiviruses that can be helpful to treat a computer from a Sality.



Also, it was detected in process monitor, action history of virus. This file virus mostly worked with registry keys. In process tree it is shown subtrees of 4.exe



**Sality** is the classification for a family of malicious software which infects files on Microsoft Windows systems. Sality was first discovered in 2003 and has advanced over the years to become a dynamic, enduring and full-featured form of malicious code. Systems infected with Sality may communicate over a peer-to-peer (P2P) network to form a botnet for the purpose of relaying spam, proxying of communications, exfiltrating sensitive data, compromising web servers and/or coordinating distributed computing tasks for the purpose of processing intensive tasks (e.g. password cracking). Virus injects as a child process when it is starts.

Complete virus treatment:

1. Launch the SalityKiller utility with the -kjax keys. This will delete the autorun.inf files in the root of the drives, restore the ability to boot in Safe Mode, disable autorun on all drives, and restore the ability to show hidden and system files.
2. Run registry editor before SalityKiller starts check Hard drive and according to the virus description, go to the [HKCU \ Software] registry key and make sure that there is no <user\_name> key 914. If so, delete this section. Next, go to the registry branch [HKLM \ System \ CurrentControlSet \ Services] and CAREFULLY search for the names of services consisting of a random set of letters.
3. Reboot in safeboot
4. Run SalityKiller again to check all files.

In conclusion, virus classification name is Sality it can be deleted by the antivirus programs, for example in virustotal shown that Kaspersky can be useful, especially it is a SalityKille from Kaspersky, also it is useful win32/SALITY remover from AVG.