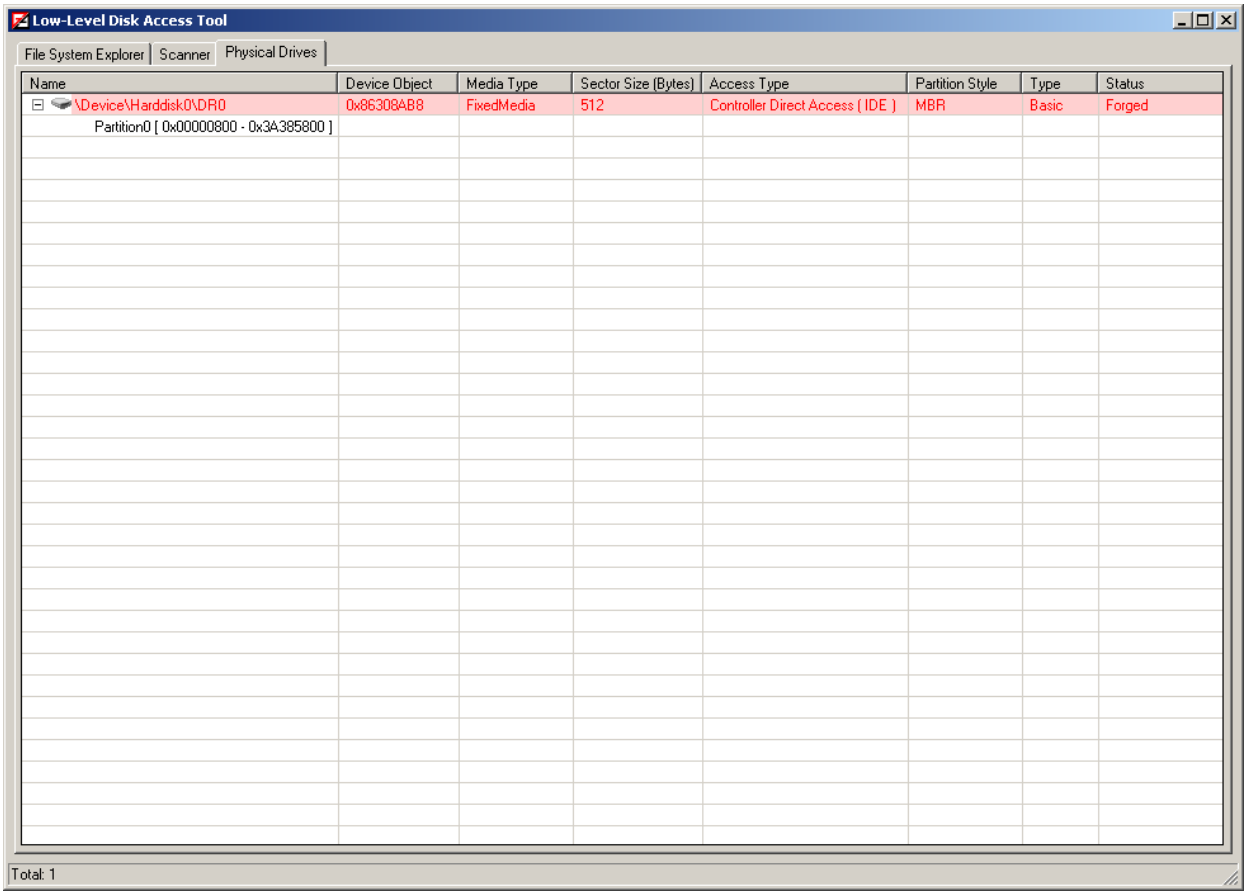
Vba32 AntiRootkit vs TDL 4

Dmitry Varshavsky
Nikolay Moskalenko

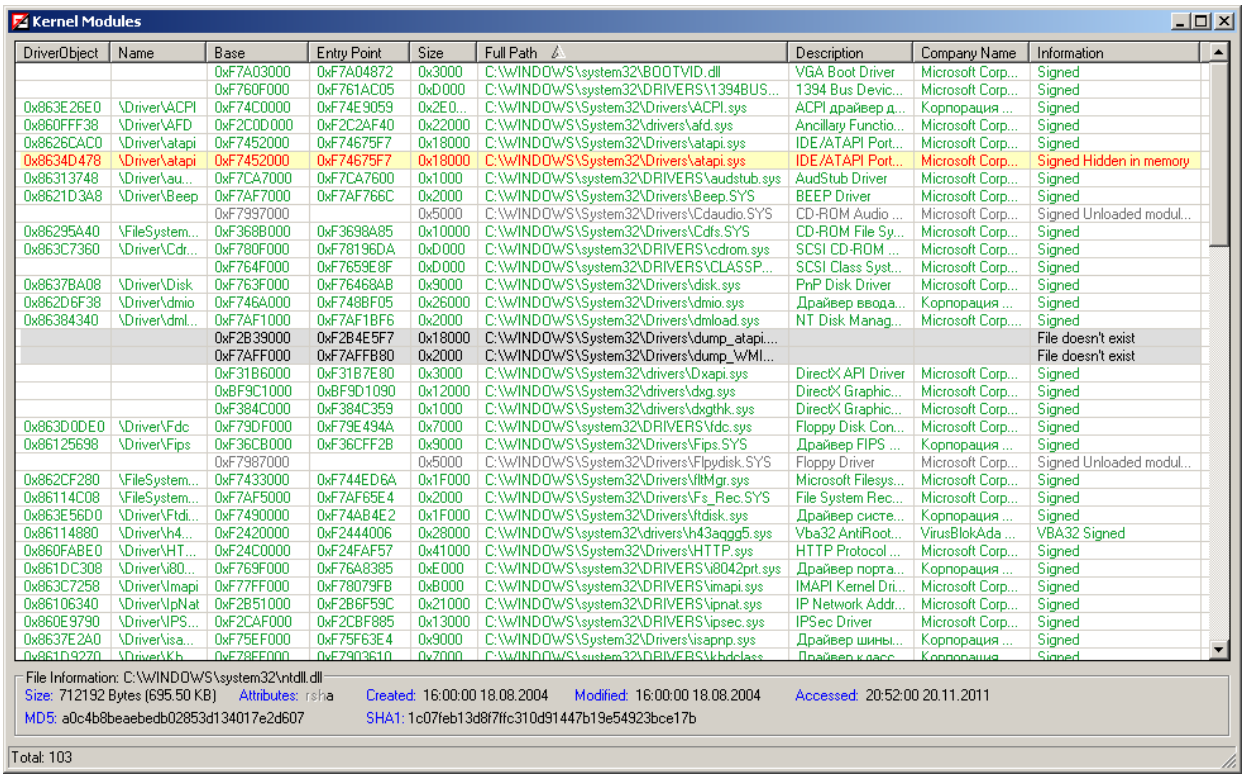
VirusBlokAda

1.Detection

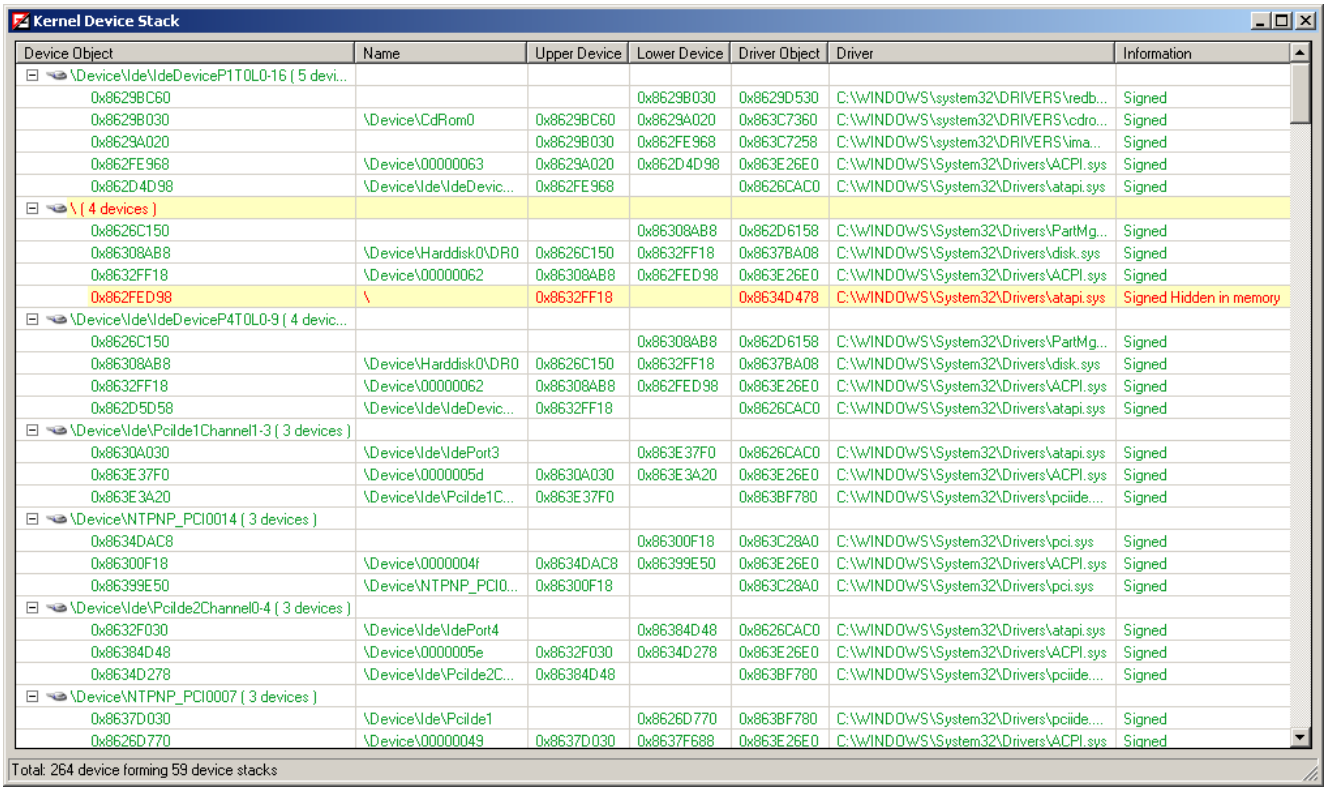
a) Forged Master Boot Record



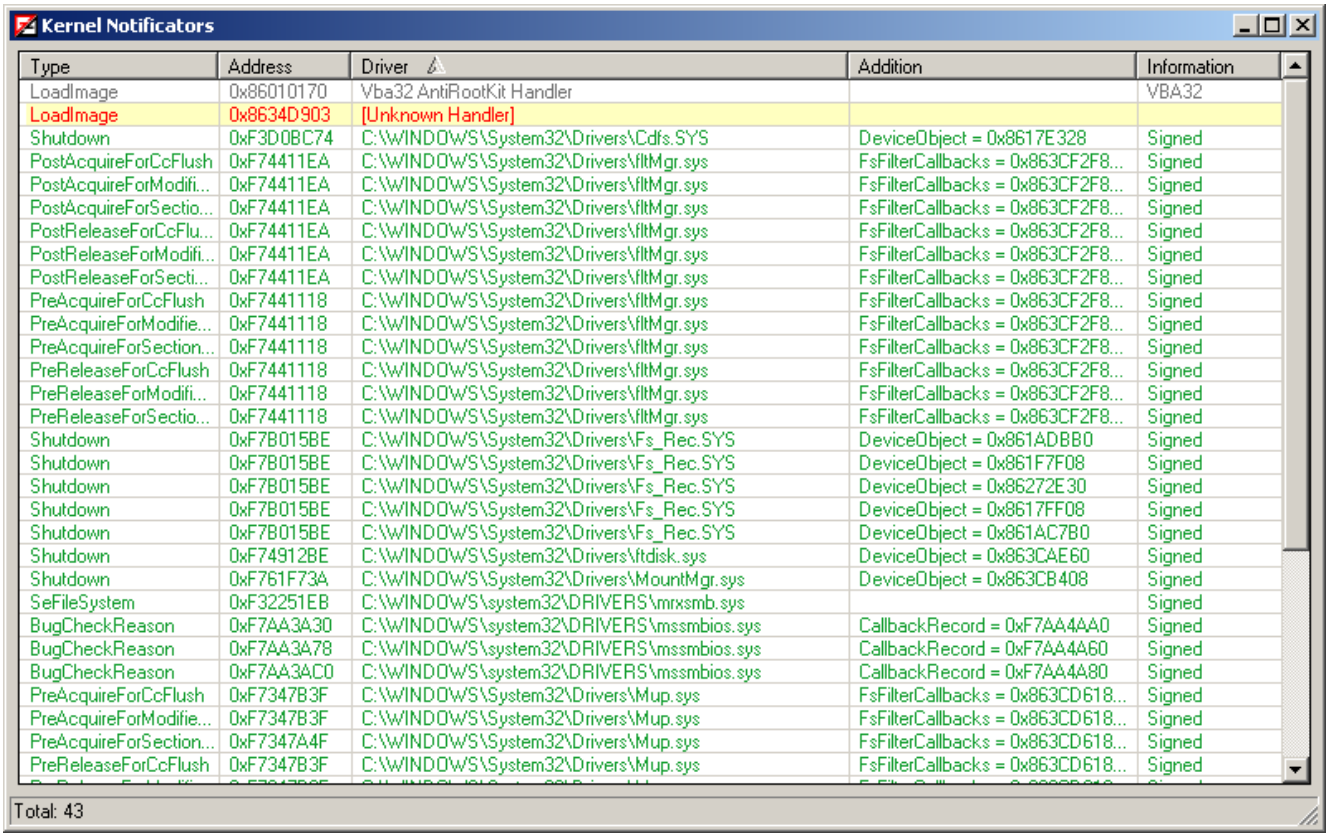
b) Additional hidden in memory atapi instance (depending on configuration it may also be iastor/scsiport/etc.)



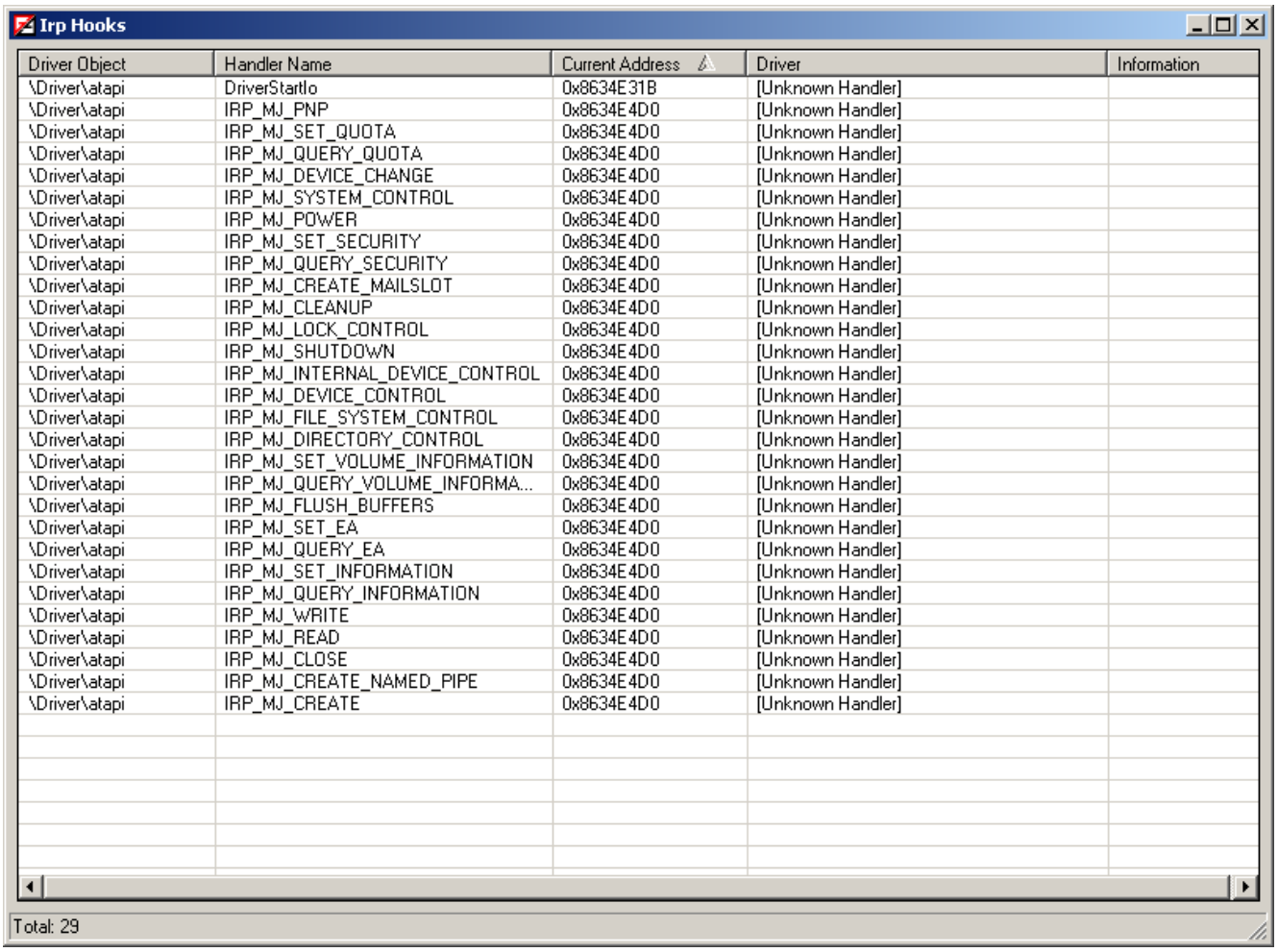
c) "\Device\HardDisk0\DR0" device stack



d) LoadImage handler doesn't belong to any loaded kernel module



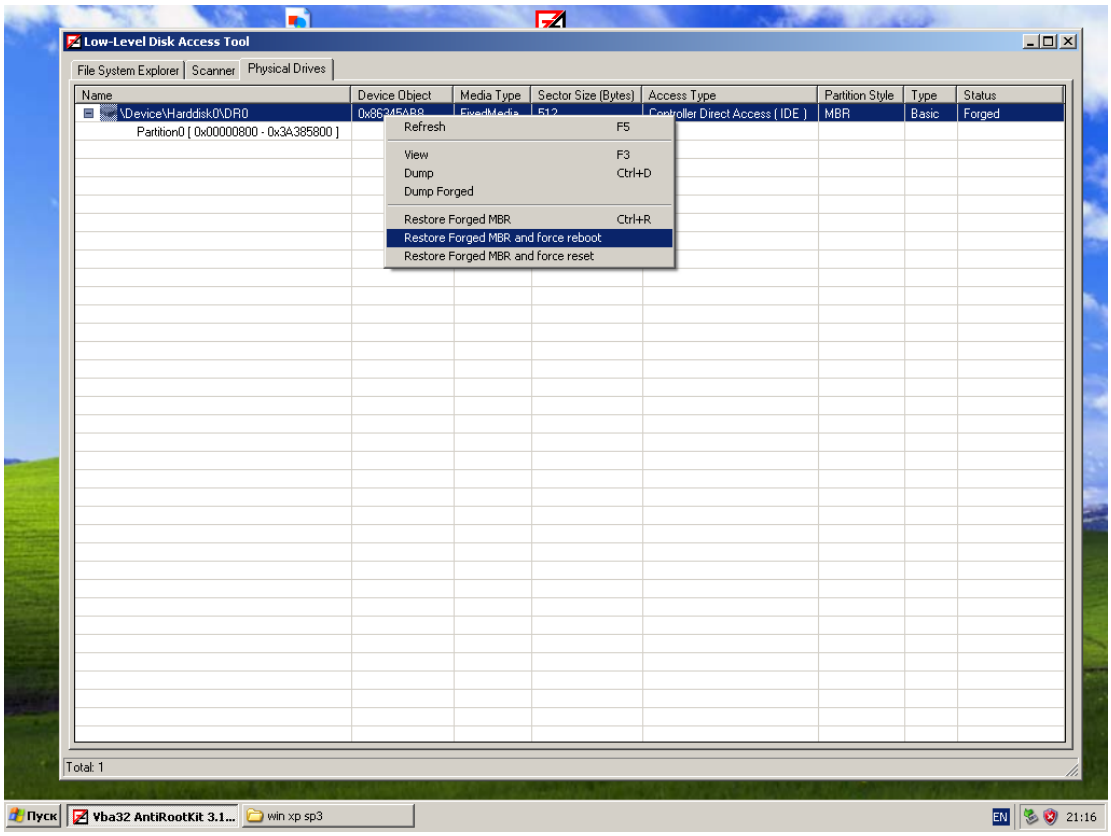
e) All of major IRP Handlers points to the same memory address



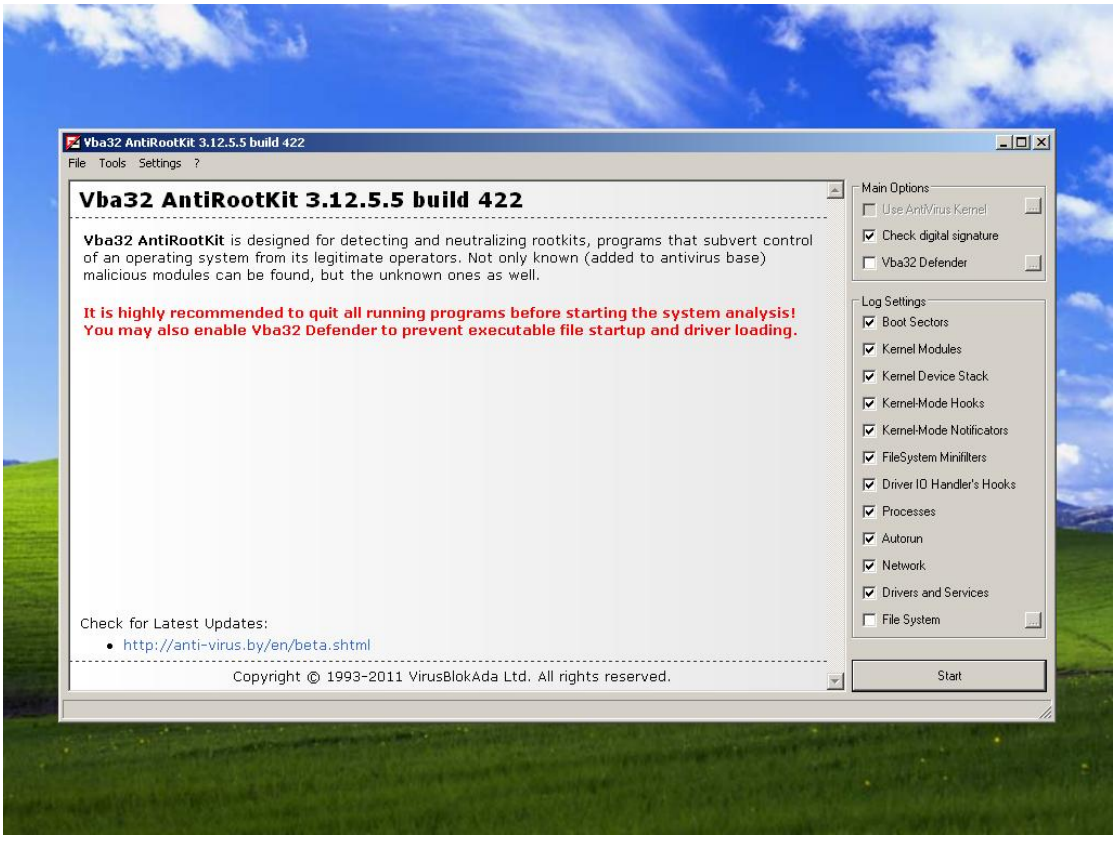
f) Note that some additional anomalies, such as injected .dlls or remote threads, which are not shown in this document, may be present in infected system

2.Removal

a) To fully disinfect the operating system select "Restore Forged MBR and force reboot" option



b) After reboot Vba32 AntiRootkit will start automatically



c) Ensure that MBR is clean and there are no other anomalies present