* HOW TO USE A.T.R.T
* HISTORY

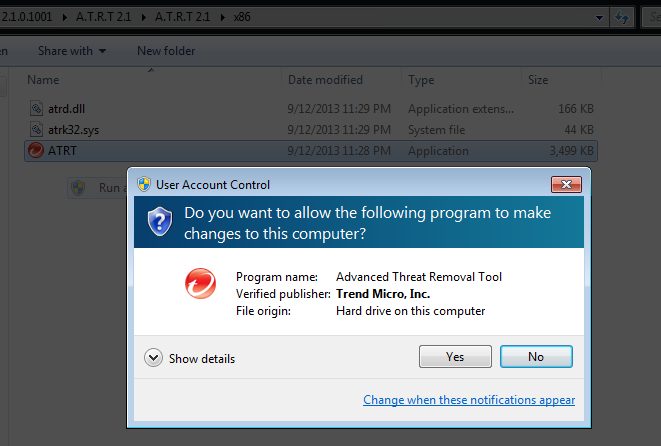
How to use A.T.R.T

1. A.T.R.T 2.1.0.1001 now support:
2. XP SP2/SP3 (32/64 bit)
3. Windows 2003 (32/64 bit)
4. Vista SP1/SP2 (32/64 bit)
5. Win7 SP0/SP1 (32/64 bit)
6. Win8 (32/64 bit)
7. A.T.R.T 2.1.0.1001 now can detect and clean bootkits and infection-rootkits as follows:

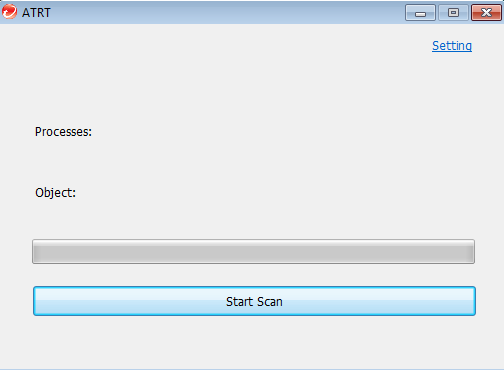
|  |  |  |  |
| --- | --- | --- | --- |
| Virus Name | Virus Type | Verify with Sample | Comments |
| Rootkit.Boot.Phanta.b | Bootkit | Y |  |
| Rootkit.Win32.TDSS.tdl4 | Bootkit | Y |  |
| Rootkit.Boot.Cidox.a | Bootkit | Y |  |
| Rootkit.Boot.Xpaj.a | Bootkit | Y |  |
| Rootkit.Boot.Yurn.a | Bootkit | Y |  |
| Rootkit.Boot.Geth.a | Bootkit | Y |  |
| Rootkit.Boot.CPD.b | Bootkit | Y |  |
| Rootkit.Boot.SST.a | Bootkit | Y |  |
| Rootkit.Boot.Wistler.a | Bootkit | N | Have no sample |
| Rootkit.Boot.Sinowal.a | Bootkit | N | Have no sample |
| Rootkit.Boot.Nimnul.a | Bootkit | N | Have no sample |
| Rootkit.Boot.Trup.b | Bootkit | N | Have no sample |
| Rootkit.Boot.Backboot.a | Bootkit | N | Have no sample |
| Rootkit.Boot.Phanta.a | Bootkit | N | Have no sample |
| Rootkit.Boot.Phanta.c | Bootkit | N | Have no sample |
| Rootkit.Boot.Stoned.a | Bootkit | N | Have no sample |
| Rootkit.Boot.SST.b | Bootkit | N | Have no sample |
| Rootkit.Boot.Sinowal.b | Bootkit | N | Have no sample |
| Rootkit.Boot.Pihar.a | Bootkit | N | Have no sample |
| Rootkit.Boot.Pihar.b | Bootkit | N | Have no sample |
| Rootkit.Boot.Cidox.b | Bootkit | N | Have no sample |
| Trojan-Ransom.Boot.Mbro.d | Bootkit | Y |  |
| Rootkit.Boot.CPD.a | Bootkit | N | Have no sample |
| Rootkit.Boot.Plite.a | Bootkit | N | Have no sample |
| Rootkit.Boot.Qvod.a | Bootkit | N | Have no sample |
| Rootkit.Boot.Smitnyl.a | Bootkit | N | Have no sample |
| Rootkit.Boot.Harbinger.a | Bootkit | N | Have no sample |
| Rootkit.Win32.TDSS.tdl3 | Infection-Rootkit | Y | Test on some variants |
| Virus. Win32.ZAccess | Infection-Rootkit | Y | Test on some variants |

Additionally, A.T.R.T 2.1.0.1001 can scan and clean suspicious boot sectors and files, but we recommend you just skip the suspicious item and upload related results for further analysis.

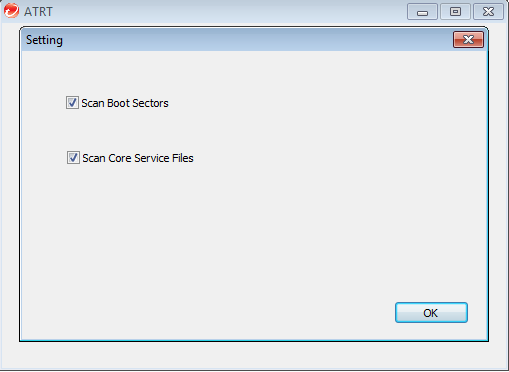
1. Run ATRT.exe as administrator if under Vista/Win7/Win8



1. Click Start to scan

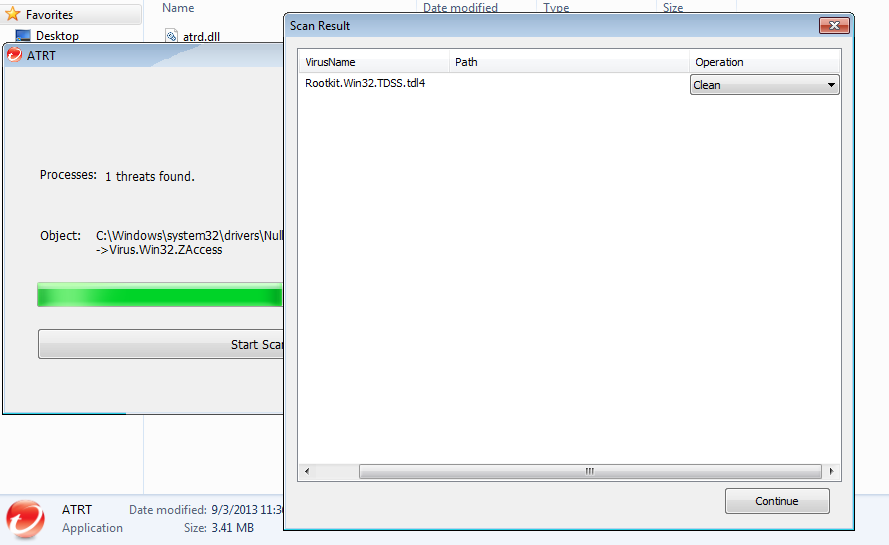


1. Optionally, click Setting

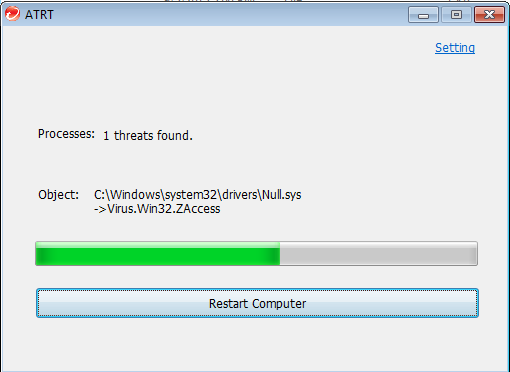


Scan boot sectors(MBR/VBR/IPL) or core service files as you want.

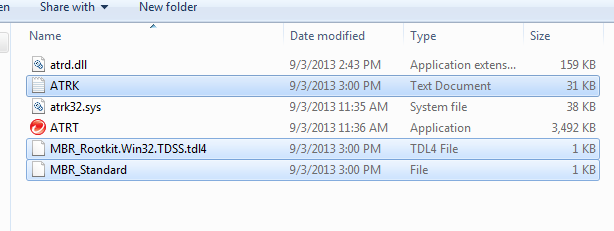
1. Choose ‘clean’ or ‘skip’ when virus/suspicious bin is found



1. Restart computer if needed



1. After clean, A.T.R.T will provide a report and dump virus binary with encryption for further analysis.



History

* A.T.R.T 2.1.0 1001

atrd.dll [1.3.0.1003]

atrk32/atrk64.sys [1.1.0.1003]

atrt.exe [1.2.0.1003]

add support for x64

* A.T.R.T 2.0.0.1000

atrd.dll [1.2.0.1002]

atrk32.sys [1.0.0.1002]

atrt.exe [1.1.1.1002]

1. fix bugs that some ZeroAccess variants under Win7 can terminate our process
2. add one more signature for ZeroAccess

* A.T.R.T 1.1

atrd.dll [1.1.0.1001]

atrk32.sys [1.0.0.1001]

atrt.exe [1.1.0.1001]

1. solve the FA:

On disk-encryption computer, ATRT will detect everything as suspicious.

1. add some message

When suspicious one is detected, the binary is requested to be uploaded.

* A.T.R.T 1.0

atrd.dll [1.0.0.0]

atrk32.sys [1.0.0.0]

atrt.exe [1.0.0.0]

create

If any question, please feel free to contact me by e-mail( Juwei\_lin@trendmicro.com.cn)