

Forum:[Hack Forums](#)

Thread: [Not used Rats in 15 years, can someone update me on startup methods](#)

lostandfound - February 12, 2020, 2:51 am

Hi - Ive not used rats for a long time, I used to use a private version of Bifrost a long time ago maybe 15 years.

When I used to use them there was the option of buying a private one as I did with Bifrost and it was not picked up by virus checkers or getting a public one and crypting it.

It seems now the only way to go is with the crypting option but there used to be a flaw in this which I am trying to understand.

For lack of a better term "in the olden days!" if you used a cryptor that would allow you to pick start up methods but the rat also had its own option for startup methods. If you went with the cryptors start up methods then you did not use the rats individual start up methods as the cryptor would manage starting it, however, if you did this you could not use the "remove" option within the rat or when the rat updated you could not use the "update stub" as the startup was managed by the cryptor.

Is this still an issue now? Whats the best way to manage startups with rats which need to be crypted?

Thanks

Aekras1a - February 13, 2020, 1:46 pm

Code -----

1. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\

All values in this key are executed.

2. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce\

All values in this key are executed, and then their autostart reference is deleted.

3. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices\

All values in this key are executed as services.

4. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce\

All values in this key are executed as services, and then their autostart reference is deleted.

5. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\

All values in this key are executed.

6. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\

All values in this key are executed, and then their autostart reference is deleted.

7. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\Setup\

Used only by Setup. Displays a progress dialog box as the keys are run one at a time.

8. HKEY_USERS\.Default\Software\Microsoft\Windows\CurrentVersion\Run\

Similar to the Run key from HKEY_CURRENT_USER.

9. HKEY_USERS\Default\Software\Microsoft\Windows\CurrentVersion\RunOnce\
Similar to the RunOnce key from HKEY_CURRENT_USER.

10. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
The "Shell" value is monitored. This value is executed after you log in.

11. HKEY_LOCAL_MACHINE\Software\Microsoft\Active Setup\Installed Components\
All subkeys are monitored, with special attention paid to the "StubPath" value in each subkey.

12. HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\
All subkeys are monitored, with special attention paid to the "StaticVXD" value in each subkey.

13. HKEY_CURRENT_USER\Control Panel\Desktop
The "SCRNSAVE.EXE" value is monitored. This value is launched when your screen saver activates.

14. HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager
The "BootExecute" value is monitored. Files listed here are Native Applications that are executed before Windows starts.

15. HKEY_CLASSES_ROOT\vbsfile\shell\open\command\
Executed whenever a .VBS file (Visual Basic Script) is run.

16. HKEY_CLASSES_ROOT\vbefile\shell\open\command\
Executed whenever a .VBE file (Encoded Visual Basic Script) is run.

17. HKEY_CLASSES_ROOT\jsfile\shell\open\command\
Executed whenever a .JS file (Javascript) is run.

18. HKEY_CLASSES_ROOT\jsefile\shell\open\command\
Executed whenever a .JSE file (Encoded Javascript) is run.

19. HKEY_CLASSES_ROOT\wshfile\shell\open\command\
Executed whenever a .WSH file (Windows Scripting Host) is run.

20. HKEY_CLASSES_ROOT\wsffile\shell\open\command\
Executed whenever a .WSF file (Windows Scripting File) is run.

21. HKEY_CLASSES_ROOT\exefile\shell\open\command\
Executed whenever a .EXE file (Executable) is run.

22. HKEY_CLASSES_ROOT\comfile\shell\open\command\
Executed whenever a .COM file (Command) is run.

23. HKEY_CLASSES_ROOT\batfile\shell\open\command\
Executed whenever a .BAT file (Batch Command) is run.

24. HKEY_CLASSES_ROOT\scrfile\shell\open\command\
Executed whenever a .SCR file (Screen Saver) is run.

25. HKEY_CLASSES_ROOT\piffile\shell\open\command\
Executed whenever a .PIF file (Portable Interchange Format) is run.

26. HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\
Services marked to startup automatically are executed before user login.

27.
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Winsock2\Parameters\Protocol_Catalog\Catalog_Entries\
Layered Service Providers, executed before user login.

28. HKEY_LOCAL_MACHINE\System\Control\WOW\cmdline
Executed when a 16-bit Windows executable is executed.

29. HKEY_LOCAL_MACHINE\System\Control\WOW\wowcmdline
Executed when a 16-bit DOS application is executed.

30. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit
Executed when a user logs in.

31.
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad\
Executed by explorer.exe as soon as it has loaded.

32. HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\run
Executed when the user logs in.

33. HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\load
Executed when the user logs in.

34. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\run\
Subvalues are executed when Explorer initialises.

35. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\run\
Subvalues are executed when Explorer initialises.

Code Folder Autostart Locations

1. windir\Start Menu\Programs\Startup\
2. User\Startup\
3. All Users\Startup\
4. windir\system\iosubsys\
5. windir\system\vm32\
6. windir\Tasks\

File Autostart Locations

1. c:\explorer.exe
2. c:\autoexec.bat
3. c:\config.sys
4. windir\wininit.ini
5. windir\winstart.bat

6. windir\win.ini - [windows] "load"
7. windir\win.ini - [windows] "run"
8. windir\system.ini - [boot] "shell"
9. windir\system.ini - [boot] "scrnsave.exe"
10. windir\dosstart.bat
11. windir\system\autoexec.nt
12. windir\system\config.nt

Enjoy ^^

Martyrdom - February 18, 2020, 4:11 am

(Feb 13, 2020 02:46 PM)Aekras1a Wrote: [\[CITE\]](#)

Enjoy ^^

Very quality, direct answer.