Subject: Re: Ransom Ware
Posted by Wayne Parham on Fri, 20 Jul 2012 03:22:50 GMT
View Forum Message <> Reply to Message

I've been running a program called "UnHackMe" for about five years now. I got a copy after first encountering rootkits, and I have had several occasions where it has saved a computer, and one time where it brought one back from the dead.

It's a sort of clunky looking program, but it works well. It was obviously written by Russians, and at first that may make you suspicious, but it is good software.

If it is installed on a system with a rootkit, it will shut everything down, not even giving a screen for several minutes. The program authors were bad about not giving feedback in that case - because you think you've totally hosed the computer when it happens. But after what seems an eternity, it awakens from its slumber to run the install program. It has eradicated the rootkit and started putting things back together again.

In most cases, when installed on a healthy PC, you won't really notice anything from it. Except when new updates are installed, in which case the next time you boot the computer, it will annoyingly tell you about everything that has changed and ask you to confirm it or roll it back. It's a long process to single-step through, but it does ensure that only what you want gets in. And it helps you identify whether those cryptic processes are valid or not, by showing you what the service is trying to do, and who wrote it. It even gives an estimate of whether or not it is legitimate. It even suggests some places to look up the questionable process, if you are really unsure about a newly installed process.
UnHackMe