Subject: Re: Ransom Ware
Posted by Thermionic on Fri, 20 Jul 2012 03:13:15 GMT
View Forum Message <> Reply to Message

Bruce, what you got hit with was a rootkit. They were an epidemic a few years back when I serviced computers, that I had to deal with continuously. They're insidious beasts that practically no big-name commercial anti-virus programs can stop completely once they've sunk their fangs in.

In geek-speak, the 'root' in rootkit means the base drive, administrator account, directory, etc on a computer. The 'kit' part refers to their 'installation kit', normally a fake anti-malware scanner. The kit exploits the normal operational functions within a web browser, that unfortunately also double as security vulnerabilities in the hands of those with less-than-sterling morals. Those who take the bait and buy the "fix" are not only out 75 bucks immediately, but thieves immoral enough to write the rootkit in the first place now have possession of their credit card number. And, your computer gets even more malware downloaded and installed in the process.

There are two main categories of rootkit, which are user-mode and kernel-mode.

Windows is configured with 'heirarchical protection domains', which are a mechanism meant to protect the OS from catastrophic failure if a few non-critical files are corrupted or deleted, such as in the cases of malware infestation or minor hard drive damage. Protection domains can be thought of as four concentric rings, which are numbered 3, 2, 1, and 0 from outermost to innermost.

Windows guest accounts reside in Ring 3, and of course have no privileges to change settings or access certain files. Regular user accounts reside in Ring 2, and have limited privileges. Administrator accounts reside in Ring 1, and can do anything except modify or delete protected system files. Finally, Ring 0 is the Windows operating system's core, called the 'kernel'.

The user-mode rootkit installs itself in the outer rings (the 'Windows user' rings, hence the name), and therefore can't really totally trash your computer; it just makes you THINK it has. It blocks all your legitimate anti-virus/spyware programs from opening, and pretty much every other piece of software on your computer as well, including the web browser. The ensuing panic causes many to fork over their credit card number, which unlocks your computer but leaves it running slower than a drunk pig because of all the spyware it has installed. Generally, these user-mode kits aren't too hard to get rid of in Windows Safe Mode, if you know which software to use and how to use it. You often have to manually restore a few settings it has changed, but it's usually nothing major. So often, a user-mode 'kit's bark is worse than its bite.

On the other hand, a kernel-mode 'kit installs itself in the actual Windows kernel. These babies therefore have unfettered access to ANY file on the hard drive, and can change or delete any file or registry key, without restriction. They're also nearly impossible to detect with anti-rootkit software, much less remove. When one of these takes up residence at 1 Windows Drive, Apartment C:\, you can pretty much figure that formatting your drive and starting over with a fresh, new copy of Windows is your only recourse for complete relief.

In short, when a user-mode 'kit moves in, you can run it out of the house with the appropriate

weapons, and effect do-it-yourself repairs to fix the damage to the carpet and walls. But when a kernel-mode 'kit moves in, YOU must leave the house and burn it behind you to kill the rootkit, then build a new house from the ground up.

Thermionic
