Subject: Ransom Ware
Posted by gofar99 on Sat, 14 Jul 2012 21:43:57 GMT
View Forum Message <> Reply to Message

Hi Everyone, Just a had a new experience. Two days ago my pc was hijacked by ransom ware. What happens is an intruder encrypts some key files and makes it so it looks like a hard drive failure. Nothing will work except the message they post saying they can fix it and where to send money. No files are actually erased, just everything is encrypted and not accessible. So what happens if you send the money.... my guess is they fix it for a while and then screw you again and oh by the way, now have a link to an account that you sent money from. There are programs to get rid of the infection, but they can't un-encrypt the files.

It had been several years and lots of junk was in the pc so I did a clean rebuild. Fortunately nearly anything I cared about was already off loaded. Very few things were lost in the process. But have you any idea how many updates there are to windows XP Pro? (I use it on this pc to run programs that won't run in win 7 - or at least don't like to run under a virtual disk). There were 169 updates. Fix some and then there were fixes to the fixes. Gads.

BTW the site to "fix" the PC showed up as www.file-recovery-software.com and the money would go to OnPay, INC (US). If you see that site pop up you are screwed.

Subject: Re: Ransom Ware
Posted by Wayne Parham on Sun, 15 Jul 2012 05:28:03 GMT
View Forum Message <> Reply to Message

Yeah, I hate that kind of malware. Once you hit one of those sites with the fake virus scanners, the trojan is off and running. Most of the malware scanners will catch 'em and jail them, preventing them from doing any harm. But if your PC doesn't have a current virus program running, it is sometimes pretty hard to fix the damage afterwards.

Subject: Re: Ransom Ware
Posted by gofar99 on Mon, 16 Jul 2012 01:10:42 GMT
View Forum Message <> Reply to Message

Hi All, I was running current virus software, two different malware checkers, a firewall and the provider also has a firewall and uses McAfee. I suspect the link to the PC came through an email - one without an obvious external link.

Subject: Re: Ransom Ware
Posted by Wayne Parham on Mon, 16 Jul 2012 12:44:10 GMT

View Forum Message <> Reply to Message

Wow, that's amazing. None of the virus scanners caught it, huh? Must've been a new one they didn't have in their databases yet. Damn! That's the worst!

Subject: Re: Ransom Ware
Posted by love2play on Tue, 17 Jul 2012 01:20:18 GMT
View Forum Message <> Reply to Message

This happened to me on Facebook and I had up to date Norton virus protection on. The virus even looked like a Norton mesasge at first. I ended up having to take my computer down to factory to get rid of it. I had it happen again on another site, and as soon as the message popped up I turned the computer off. When I turned it back on the virus protection caught it and took care of it.

Subject: Re: Ransom Ware
Posted by gofar99 on Tue, 17 Jul 2012 01:53:53 GMT
View Forum Message <> Reply to Message

Hi, this one was too fast. As soon as it hit.... there were a full screen full of windows error messages. Then it popped up the "fix it" screen.

Subject: Re: Ransom Ware
Posted by LuvMartin on Thu, 19 Jul 2012 01:55:51 GMT
View Forum Message <> Reply to Message

I have had one of these too and I also had to take the computer back down to factory settings to get rid of it. Technology is great until you can't use it!

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

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

Subject: Re: Ransom Ware
Posted by gofar99 on Fri, 20 Jul 2012 14:47:20 GMT

View Forum Message <> Reply to Message

Hi, Twas certainly a rootkit that was kernel based. I had the same thoughts on the pay to get it fixed. No way! Rootkiller found it and got it out, but the file structure etc was still encrypted. So I reformatted it and made a clean load. Thanks for the information I am sure it will help others too. Stuff like this has made me nearly want to switch to Linix. I did once and while it was just fine as an operating system, some software I wanted to run was not available (nor anything similar).

Subject: Re: Ransom Ware
Posted by Wayne Parham on Sat, 21 Jul 2012 15:43:46 GMT

View Forum Message <> Reply to Message

I'm with you there, Bruce.

I prefer Linux, and develop C/C++ applications that run on Ubuntu (for dev and test) and RedHat linux (for production). The server that runs AudioRoundTable.com is Gentoo.

For personal use, I run Ubuntu on one of my laptops. It is stable and user-friendly. Whenever anyone visits and needs to borrow a computer, that's the one I give them. It's perfect for surfing the web or typing documents (OpenOffice is compatible with Word and Excel).

But, yeah, I still have a few boxes running Windows. All XP or Vista though. Not gonna move off those.

Slightly off-topic, but I don't see many people (certainly no companies) moving to Windows 8. It's basically a device (phone/tablet) operating system put on the desktop.

Subject: Re: Ransom Ware
Posted by gofar99 on Sat, 21 Jul 2012 18:13:36 GMT
View Forum Message <> Reply to Message

Hi Wayne, I down loaded a copy of "Puppy Linux" today. It was on the web - a security site. It was on how to do on line banking with a live CD of Linux. It does indeed work, but I would need to make a second disk with the correct settings for connecting to the web etc. It would be a pain to have to go through all the gyrations every time. I'm not sure how to do that in Linux so it may have to go on the shelf until I get to it. I have two desktops on XP Pro and a laptop with Win 7 (with a VM for XP Pro). No Vistas and no chance for 8. A fix for a problem I don't have.

Subject: Re: Ransom Ware
Posted by Wayne Parham on Sat, 21 Jul 2012 18:24:14 GMT
View Forum Message <> Reply to Message

Check out Ubuntu.

Subject: Re: Ransom Ware
Posted by Thermionic on Sun, 22 Jul 2012 01:08:03 GMT
View Forum Message <> Reply to Message

I'll likewise cast my vote for Ubuntu; very well thought, stable, fast, and a nice change from Windows. I set up the 'puter I'm using right now as a dual-boot machine with XP and Ubuntu. However, there's the problem Bruce mentioned, of program and driver compatibility. But, that's changing for the better every day.

While on the topic of Linux, most ASUS motherboards these days come with "Express Gate," which is a built-in miniature Linux operating system with an OS X-like GUI. It's up and running in just a couple of seconds after the BIOS splash screen, and you can surf the web, check e-mail, view photos and files on your Windows file system, etc. You can be on the Web in literally 10 seconds after hitting the power button!

To use it, just click your mouse when it comes up. Or, do nothing and in a few seconds (the timer is BIOS-adjustable) it'll shut off and the Windows bootloader will start. I've built many computers with it, and some love it while others want me to turn it off for them. Personally, I think it's pretty cool. As one who doesn't leave their computer on all the time, it's VERY nice for when you wanna look something up really quick, or show a visitor some pics. No more waiting to boot into Windows just to do a small task.

Thermionic