SECURITY NOW!

Transcript of Episode #129

Windows SteadyState

Description: Steve and Leo examine and discuss Microsoft's "Windows SteadyState," an extremely useful, free add-on for Windows XP that allows Windows systems to be "frozen" (in a steady state) to prevent users from making persistent changes to ANYTHING on the system.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-129.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-129-lq.mp3

INTRO: Netcasts you love, from people you trust. This is TWiT.

Leo Laporte: Bandwidth for Security Now! is provided by AOL Radio at AOL.com/podcasting.

This is Security Now! with Steve Gibson, Episode 129 for January 31, 2008: Windows SteadyState. This show and the entire TWiT broadcast network is brought to you by donations from listeners like you. Thanks.

It's time for Security Now!. Steve Gibson is here, the security guru from GRC.com. That's where you'll find, of course, SpinRite, his great program for disk maintenance and recovery, but also all those free security programs he's written over the years. And our podcast, GRC.com. Hello, Steve.

Steve Gibson: Hey, Leo. Great to be back with you. As a consequence of the fact that you are actually in Vancouver right now as our listeners are listening to this, we recorded this episode #129 immediately after #128.

Leo: A week ago.

Steve: Exactly, a week ago. Consequently, I have not had a chance to have a week's worth of what has happened in security happening between now and then. So I do not have any news for security. However, when we record next week's Security Now!, which is actually two weeks from time we're recording this one and one week from the time people are hearing this one, why, we'll catch up so that no one misses anything and we don't miss talking about anything that was significant.

Leo: Well, with any luck, nothing bad happened, and we didn't miss anything.

Steve: Exactly.

Leo: Although that's unlikely. But...

Steve: We're going to talk, as we mentioned at the end of last week's episode, about Windows SteadyState. And in a sort of a bizarre coincidence, I wanted to share a listener's experience with SteadyState who also shared with me his experience with SpinRite. So I thought I'd start off by sharing with our listeners - I believe Jim's last name is pronounced Gaydusek. Anyway, the subject of his SpinRite note was "SpinRite Is King."

Leo: I like that.

Steve: He says, "Hello, Steve. Let me first start off and say that SpinRite is a definite tool for any technician's toolbox. It has helped me save a few systems. One in particular, the hard drive that was all but lost. It was a friend's neighbor's system, and they have all their financial data on it, as well as personal info. They supposedly had tried everything, and even took it to some of the name brand stores, and everyone stated that the drive was toast. As a last resort, they brought this machine in. And since I have the software, I tried it on this system.

"The system ran for four days straight. You would think it was a lost cause after the workday was over. But the next day SpinRite had moved a little forward, so we waited. After the fourth day it stated that it was ready. SpinRite said it had found some corrupted sectors and possibly some unrecovered data, but had recovered others. But as we rebooted the machine, it booted up without even showing any signs of an issue. The system worked like it was new, and as far as I know to this day is still working. And this was a year and a half ago."

Leo: That's kind of neat. People ask me that, well, you know, they call in on the radio show and they say, you know, something that obviously sounds to me like a drive is - something's gone wrong with a drive. And they say, well, should I just throw it out? Is it safe to format and reinstall Windows? And the truth is, if you have SpinRite, you don't have to ask that question. You just run SpinRite.

Steve: Right. He concludes, saying, "Thank you for a truly remarkable product that has saved many heartaches, and I am sure headaches, as well. This is one I suggest to everyone I talk to who wants to know how to protect their hard drives and keep them in top working order." And he signs it, "Your loyal customer, Jim Gaydusek, Shelley School District..."

Leo: Oh, neat.

Steve: ..."Senior Tech and Network Admin."

Leo: See, that's really who needs SpinRite. Anybody who has multiple systems that they have to maintain, then it's a no-brainer.

Steve: You certainly get a lot of bang for your buck that way.

Leo: That's just a no-brainer. All right. Let's talk about SteadyState. Now, how did this come up? We talked about it a couple of weeks ago; right?

Steve: Yeah, I don't really remember. Well, for one thing, I ended up...

Leo: It was a question.

Steve: I ended up stumbling on it maybe a month ago because I was trying to configure a system for a friend who was in a corporate environment. She's an entrepreneur, wanted to set up a small network. However, in the past she had the experience of hiring employees who immediately, after sitting down at their machine, started changing them. You know, they would install their QuickBooks app because they wanted to do their personal check register on their work machine. Or they would install iTunes so that they could update their iPods. I mean, just basically they took for granted the fact that this machine was just like their machine at home and had no more respect for it than their machine at home. And before you knew it, it was infested with spyware and malware. It wasn't working right. Corporate apps wouldn't function any longer. And so she said to me, what can I do to prevent this from happening?

So interestingly, Jim in Shelley, who we found at the end of that note is the school district senior tech and network admin, he wrote a note to me about Windows SteadyState because we had mentioned it before. I thought it would be fun to kick off our discussion of this with Jim's experience. He says, "Hello, Steve and Leo. First of all, thank you from the tech community for creating a show such as Security Now!. On your last show, #127, Steve talked about SteadyState from Microsoft. And I wanted to let you know that we use it here in our libraries, and it has been a godsend. Before that, we had Windows 98 systems in the library, and always, always had problems with students messing up the works by doing whatever they wanted. It was a nightmare. Always, every other day, we were in there working on systems and restoring them or ghosting them back to their original state or removing any and all printers except the one that is supposed to be installed on them.

"Then we upgraded the machines to XP in our high school. I also had another system in my middle school library called Xtenda, which is a hardware facility that allows you to have up to four sets of I/O running off one machine. I had the SteadyState predecessor on there as well, along with the Xtenda hardware and setup, and it works wonderfully. So now that I have XP in our high school, I'm able to use the new Windows SteadyState. It took some working to get it working properly on the system without enabling the hard drive locking feature, but it is working. I had to do a registry hack to keep the wallpaper from changing, but it works like a charm.

"The only problem I have had with it is that at one point there was an issue with system updates because it would lock the user profiles and not allow anyone to log on. But after a number of reboots the systems were all back online and updated. No real info on that problem on Microsoft's help site, but people with the same problem indicated that it just seemed to clear itself up. As for the systems, they all now run wonderfully.

"I would suggest, though, to have a good machine to run this software. The machines this is running on are slow Celerons with only 512MB of RAM. The problem we ran into is that when you enable the system to lock the hard drive, it essentially makes a copy of the entire hard drive to a sort of swap file. Then if you reboot it puts that image back to its restored state. If you shut down and reboot, it takes about five to eight minutes to come up to a log-in screen because it has to recreate that image. In a school environment, that's a little long for our taste. And that's why I do not have that feature enabled. But it still has enough additional features to safely lock the system to ensure no changes can be made to it.

"So those are just my thoughts on SteadyState and how we use it here. Thanks for listening."

Leo: So it can be used two ways. It can kind of be a policy editor, as well as a way of getting everything back to the original state.

Steve: Yes. I don't know how many of our listeners have ever messed around in what's called Windows Group Policy, or with the group policy editor. But there are a phenomenal number of settings which are accessible. GP Edit is the name of the group policy editor. If you just go down to your Run line under the Start menu and put gpedit.msc, it's not an EXE, it's an MSC file extension that will run the group policy editor, where you can then begin to browse around and see just a phenomenal number of things that are in there.

One of the problems with the group policy editor is that many of the functions interact with each other, and they're really not very well documented. It's almost like you have more control than you want, and essentially more responsibility than you want or perhaps need. So one of the things that Windows SteadyState has done is it's surfaced, I would argue, the most useful things for this particular application.

So let's back up a little bit and talk about what this Windows SteadyState is. First of all, we have a link in our show notes for this Episode 129 to Microsoft's page. If you just Google "Windows SteadyState," all one word for SteadyState, it'll take you immediately to Microsoft's page where they talk about this. They have it under their shared computing sort of environment or discussion because that's really how they think of this thing. And certainly that's one of the applications. It's what our listener Leo from last week was asking.

Leo: The 16 year old who had - he was the IT manager for his house.

Steve: Exactly. And so he wanted to be able to create a guest computer, or at least use his downstairs machine, when it's not busily sucking down torrents over the Internet, he wanted to be able to allow his mom and dad to use it, but prevent them from messing it up in any fashion. And the same goes with a guest logon. So he was wondering if SteadyState would be appropriate for that. Well, it's perfect for that. It was essentially designed for that. The idea is that there is a hard drive protection technology which is built in.

Now, it's not quite as onerous in my experience as Jim's letter indicates because it does not make an entire copy of your system partition and/or drive. Instead you set aside a block of hard drive space. And using a feature, basically it's file system filtering, this is able to capture any changes which are made to the system drive. And essentially it caches the changes. So, for example, when any application, installer, literally anything you do, I mean, this thing is global. You cannot turn it off without restarting Windows. So it's not something that just sort of easily comes and goes. I mean, this is meant to be bulletproof.

And I discovered the hard way that it even protects the partition table, and that first track of the drive which we were talking about recently could be prone to preboot kernel rootkits. I was using something else that did deliberately change that first track, very much in a kernel rootkit fashion. And that'll be the subject of an upcoming podcast because it involves performing whole drive encryption. And it turns out that SteadyState uninstalled this thing, even though I had SteadyState sort of in a mode where it was supposed to allow changes to be saved. So, I mean...

Leo: That's good behavior. That's kind of what you wanted in that case; right?

Steve: Oh, exactly. I mean, if you got a preboot partition table and, you know, sort of outside of the partition virus, this thing wipes it out. It removes it. It says, we're not letting you change it. So the point is that, at the sector level, anything that attempts to write to the hard drive, that is, to the system partition, it gets instead written into this cache region. And then any subsequent reads are first checked in the cache to see if the sector is there. And if so, they're read back from there. So essentially it sort of quarantines any writes to the hard drive. And then any reads come from there if there's been a change.

So the beauty of this, instead of putting, like, a write lock on your hard drive - which Windows won't tolerate because it's constantly updating the registry, and there's all kinds of things going on with Windows, as we know, our hard drive light is flickering there even when we're not doing anything. So instead of write-locking the hard drive, it basically sequesters any writes. And when the administrator logs off, the administrator being a special user to Windows SteadyState, it will prompt you, saying do you want me to retain these changes or flush them? A normal user, a non-administrative user, does not have access to that. There's no choice that they're able to make.

But SteadyState recognizes that an administrator may, in fact, want to run Windows Update to update patches, or want to run an AV scan, and may want an antivirus program to be able to update itself. So there are instances where, when you're logged on as administrator, you would like to flush those changes, which were cached, back into the real file system to allow them to become permanent. And so SteadyState allows you to do that.

Now, as I've been talking about it, I've been careful to say that the system partition is protected. Windows SteadyState specifically only protects the Windows drive, that is, the drive on which the system is running, it's where - typically it's your C drive, where you've got your Windows or WinNT directory. I guess it's probably going to always be Windows under XP unless you upgraded an older Windows 2000 system with a WinNT directory into XP. So it's where that directory lives. And there is no way not to protect any part of that. So again, I'm impressed from a technology and an integrity standpoint that Microsoft said, look, if we're going to protect the C drive, we're going to protect the C drive, period.

This does create a problem in the scenario I was interested in because I wanted an employee of a company to be able to make changes to their system that were benign. For example, their My Documents directory, they wanted to be able to use Microsoft Office to write documents. They want to be able to put things on their desktop. They want to be able to do things of a data nature, but not, for example, have their installation of QuickBooks or iTunes or whatever junk they bring from home to permanently alter their system.

So it turns out that it is completely possible to create another drive, for example, a D drive - I like D because it's short for "data" - and to simply drag the user's profile, drag their My Documents directory over to D, as well as their desktop. And then it's able to persist. So it turns out it's also very simple to set up a system with - it does require repartitioning. For example, if a hard drive was only dedicated to a C, you would have to chop off some space for user documents. In this case I had an 80GB drive, and I just chopped it in half so there were two 40GB partitions, figuring that, you know, 40GB is plenty for your typical office worker who's storing documents.

Leo: But you could have two drives, or multiple drives; right?

Steve: Oh, you absolutely could leave - yeah, it's a very good point. You could leave C exactly as it is, install a second physical drive, and set that up, for example, to be D:. And then Windows makes it very easy to move a user profile over to another drive.

Leo: Will it protect the stuff on the D drive as well as on the C drive?

Steve: No, and that's the point. There you don't...

Leo: I guess you don't want it to because that's your documents.

Steve: Exactly. So the user's desktop, they're able to put things on the desktop, they're able to create shortcuts and so forth. Then, beyond this, SteadyState has a whole bunch of really nice options specifically targeted towards exactly this application, locking a system down and prohibiting and limiting what users are able to do. Sometimes I find that the best way to get a feeling for the functions offered by software is just to cruise around through the menus or look at the options. So for our listeners, I have taken screenshots of the configuration screens for Windows SteadyState and put them on this episode's show notes page. So it's just the episode notes for this episode, 129, has a series of just simple static screenshots showing the various options and settings which are available.

And so on a per-user basis you're able to do many things. For example, you could require a logoff after X minutes of use, or a logoff after X minutes of idleness, which, you know, you can imagine in a library mode. You might say, hey, this computer could only be used for 30 minutes by one person. So you could force a logoff after 30 minutes of use. And that lands on a user, and their time is up. It's time to let somebody else use the computer.

Similarly, there are, in much the way that IE gives you sort of a number of different profiles - highly secure, high-medium, medium, low security - SteadyState offers the same sort of features for Windows restrictions. So it offers you various ways of restricting Windows. For example, and this is one that I like, you can prevent right-clicking in the Start menu. Right-clicking is the way, for example, in the Start menu you're able to drag things around or rename objects. You can just simply, in these options, in these extensive options, just say no, I don't want to allow that. Or I only want to allow the classic Start menu. You can do things like remove the My Documents icon. There are things you would do, for example in a library mode, that you would not do if you wanted a basically useful, friendly computer that just refused to get itself infected, refused to have permanent software installed. But one of the nice things about this, in a corporate mode, is you could install, for example, you could say, look, to your employees, if you install QuickBooks, eh, we're not happy about that. But it'll be gone in the morning.

Leo: So this is, again, this is a combination of policy editor and a kind of restore function. And this is where I'm unclear. If I can't protect the user's profile - so I guess it's a policy that's keeping him from making any changes. But it does save any changes that he's allowed to make.

Steve: Well, nothing gets saved on the C drive.

Leo: Right, I understand that.

Steve: So, yeah. So, I mean, and that's just a hard and fast rule which I really appreciate because, if they started making exceptions to that, you could imagine people would find ways around it. So if you move the profile to a different drive, then you are able to allow documents and user profile-ish things to change. So, for example, you could allow the user to change the icons that IE was showing.

Leo: I see, I see.

Steve: But there's a policy, one of the options down there in the details, for example, under Internet Explorer is prevent them from making changes to that.

Leo: So if you're using this at a hotel, and you don't want any of the user's changes to be persistent, you just make everything on the C drive.

Steve: And that's - yes, exactly.

Leo: And if you're using it at a school, where you want students to have their own individual profiles with their own individual documents, that's when you create that second partition or the second drive, because that's - and then, of course, policy is still effective, but they can presumably create their own stuff.

Steve: Exactly. And I've been playing with this now for a couple weeks. And, I mean, it's a little unnerving. I just have my - I have my habits, you know, I right-click on the desktop, and up comes a little warning saying your administrator has prevented you from making any changes on the desktop. It's like, whoa, okay, sorry. But, you know, I'm glad because I checked - one of the little checkboxes was prevent people from changing screen resolution or basically messing with the machine in a way that you don't want them to.

Leo: Right.

Steve: Anyway, it's a - I've been very impressed with it. One of the simple little checkboxes is prevent write access to USB storage devices.

Leo: Oh, fantastic.

Steve: And so just by checking that - it's funny because it caught me out, also. I use, as we've talked about, Drive Snapshot. And I was making snapshots of the C and D drive as I was going along. And so I started getting an error. It's like, wait a minute. Oh, and I think I was - I'm sure I was logged in as administrator. So even the admin user...

Leo: Oh, interesting.

Steve: Because this was global, and it requires a restart of the computer. So once again - so, yeah, I'm looking at the screen, it says "under computer restriction." So this is whole computer restrictions. And so when I realized that I had locked myself out of writing to an external USB drive, it's like, oh, shoot, I did that. So I turned it off, but it said, you've got to reboot. So again, these things are running deep in the system and are not easily circumventable. I really - to me it looks like Microsoft has done a great job.

Leo: Now, this is free. And as far as I can tell from the website it's Windows XP only.

Steve: Yes. It's XP only, first of all, because none of this technology existed back in Windows 2000. So Win2K is too old to take advantage of this. And there is language on the SteadyState pages saying that Vista incorporates enough of this that they didn't do this for Vista. I'm guilty of not knowing Vista well enough to be definitive on what features Vista offers that are like this. But with any luck, many of our listeners are still on XP.

Leo: Well, this is a good reason to stay with XP, frankly.

Steve: Leo, this is a neat tool. Yeah, I am very, very impressed with what this provides because it is simple to install. In the default configuration, where users are going to be on the system drive, that is, user profiles will be there, for example, I'm sure this is the case with the way Jim has set it up in his school libraries. You want kids to be able to use the machine, but it - I mean, he was talking about reghosting and reimaging these things in order to bring them back to sanity every morning. Here, this thing, it will allow - it's plastic while you're using it. You can do things. Things all work. But when you log off, everything you did disappears, and the system is returned to a steady state.

Leo: Now, if you're listening, like me, and saying, well, why didn't I know about this, this is fairly new. It only came out a few months ago.

Steve: Right.

Leo: So it's not like it's been around for XP all along. But I have to say, you know, I mean, here we are sitting with Vista. If you put this on your home system, you know, your home network, with XP, you'd be more secure than Vista.

Steve: Microsoft doesn't suggest that this replaces antivirus software.

Leo: But wait a minute, I mean, how could a virus infect you if you've got this running?

Steve: That's what I think, too. I think that they're just hedging their bets. They're not wanting to piss off the AV vendors, either. They've go documented compatibility with a small number of antivirus software, where SteadyState recognizes the AV you're using and is able to permit some compatibility with it in order, for example, to allow patterns to be updated. Users of specific AV software will have to take a look and see if it's automatic or not. One of the issues that Jim talked about is mentioned in the FAQ document that goes along with this, and that's relative to Windows scheduled software updates. SteadyState has the ability, for example, to run Windows Update at 3:00 a.m. if the machine is on and allow it to properly synchronize and receive Windows updates, which will then be made permanent.

Leo: Even better. So it's a kind of automatic Windows Update. It's locked down. By the way, I just sent you a link. There is a beta for SteadyState 2.5 that is Vista compatible. So they're clearly developing it for Vista. It's just it took them five years to do it for XP, and they're only now getting around to doing it for Vista. Now, this came out in November, so I have a feeling it's probably pretty stable.

Steve: I'm glad to know that because, again, there may have been features buried somewhere, lord only knows where, in Vista. But one of the things I like about this is this is just turnkey. It is easy to use. Now, one thing I had...

Leo: Who shouldn't use this?

Steve: It gets in your way a little bit. Jim mentioned the problem of starting up the machine and how long it takes to boot.

Leo: Yeah, eight minutes and all that, yeah.

Steve: Yeah. In my experience there is a pause after you log on, where I've been asking myself, okay, what is it doing? Well, it's not writing and reading the drive because I looked at the drive lights. And the drive lights...

Leo: Oh, interesting. You'd think it would just be copying all the cached stuff back onto the C partition.

Steve: Yeah. I'm not sure what's going on. But there does seem to be a pause in the process. And I thought, well, maybe it doesn't like other things that I've got set up. So I stopped services, and I experimented with it. It's when I stopped the SteadyState service that it did it then, booted right into the desktop. With the SteadyState service running in the background, there was that delay. But again, in my mind, no way was it eight minutes. It was maybe 30 seconds. And so it's like, okay, well, that...

Leo: Well, he could have older, slower computers. I mean, he may not...

Steve: Well, and in fact he did mention that those machines were slow Celeron machines with only 512MB of memory.

Leo: There you go.

Steve: Now, one thing about SteadyState is it tends to be aggressive with the size it would like to have for its cache. In the installation instructions it instructs you to defrag your drive. So of course they're trying to cram all of your used space to the front of the drive, leaving a big chunk, a contiguous area of free space. By default, it takes half of your remaining free space. Well, that's ridiculous. If you have a 120GB drive, and you've got a relatively new Windows system that maybe only has 12GB in use, you know, you don't want to lose half of that.

The good news is, you are able to tune the cache size down as small as you want. I don't really know why it just grabs half of the available space without limit, but that's what it does. There's no reason not to tune the cache size down to maybe 3 or 4GB and control how much space it's got for its cache. There is documentation that says, well, if users made lots of changes, they might get a dialogue saying they have to log off in order to allow this cache to be flushed. So but my sense is, again, it's a little bit underdocumented at this point. It's not clear to me why you'd run out of space unless you had, for example, 50GB of active space, and your cache was only a few gig, and you tried to change more than that many gig of storage.

Leo: I would think the same size as your Windows, you know, your Windows partition, you know, it should be enough.

Steve: Yeah, exactly. And so that's the assumption under which I've been operating. And I have never had it tell me that I've run out of space. And I've been pounding on it and using it. And I'm really impressed, Leo. This thing is very cool.

Leo: I'm blown away. I'm going to start recommending this. It sounds like anybody who maintains a number of systems with users that are unruly, whether it's your teenage kids or your schoolchildren or your customers in an Internet caf, this is an absolute win.

Steve: And again, I cannot under- I mean, Microsoft is saying you still need to use AV. And it's like, okay, well, I mean, you and I don't, Leo, anyway. So, I mean, it's not like...

Leo: It's belt and suspenders. They're selling OneCare, and they don't want people to not buy OneCare probably. I mean, there may be - it's possible for a virus to get around the SteadyState restrictions. We don't know how secure they are.

Steve: That's a very good point. And again, when software running in your machine is trying to protect you from other software running in your machine, we always know there's going to be a cat-and-mouse conflict there, you know, Spy vs. Spy sort of thing. But this, I mean, I'm very, very impressed. So I absolutely wanted to bring this to our listeners' attention because I'm sure, I mean, as people are listening to this, they're thinking, oh, my god, that's exactly what I need for Aunt Sarah.

Leo: I'm tempted to install it on the machines I use just to protect them so that I can't do anything dumb. And then I can always get back to a known state. You know, I mean, for instance, there's a Windows machine I use pretty much exclusively for recording and editing in Adobe Audition. That's exactly what I'd like, that I could always get back to a known good state every morning. Just reboot.

Steve: Well, and even in the case that the C drive will not change, all you have to do is either partition that into half, or use a second drive that's D. There's no protection at all on anything other than C. So that's something people have to understand, but it's also useful because it means you can have a data drive where you absolutely know SteadyState is not going to get in its way. And so you're never going to have a problem with things you thought were safe not being safe.

Leo: Well, and I've always kept a separate data drive for my Windows drive. So it's just a natural way of operating for me. So this is really neat. Now, I do remember there's a commercial program that does something similar, and I just can't remember the name of it. But I've had people tell me, you know, IT pros tell me about it, and that's what they've been using up to now. But this is free. It's from Microsoft. Seems like it's a much better solution that GP Edit.

Steve: Well, yeah. And for example, here under general restrictions, prevent autoplay on CD, DVD, and USB drives. It's just - you just click that on. And now if some smart aleck, you know, thinks he's going to get around your restrictions by using a CD - oh. There is in the FAQ a question of whether or not system would boot for a USB or a CD. And so they specifically address the fact that, yes, if you boot something ahead of Windows, it will have your machine. So in a lockdown mode you would want to also tighten down the BIOS. You would want to remove anything but the hard drive from the boot order in the BIOS and, you know, maybe turn off the CD in the BIOS if that's available. But here, you know, by just setting a checkmark, you disable autoplay.

Leo: Well, that's great. You can turn off that U3 thing. I mean, if you're in a library, man, you want to turn off U3.

Steve: Yup. I mean, here's prevent access to task manager. Oh, there's also a complete screen that easily allows you to blacklist programs. So you're able to say, for example, I do not want any of the following programs. And so this lists all the programs that you've got installed, and you simply move - you either click "Block All," or you're able to move them one by one over into the blocked programs list, and they will no longer run.

Leo: Good.

Steve: So, I mean, it makes it very simple to lock a system down.

Leo: Steve's got some great screenshots, so you can see this before you install it, and all the different settings and so forth, at his website. We'll put those show notes, the links in the show notes, and you'll have it at GRC.com/securitynow. And let's add a link to that SteadyState beta for Vista because I know there's some Vista users probably would love to have this. Although, to me, this is one more reason to stick with XP. I mean, why not?

Steve: Yes. They've done a great job with this. And I will mention that, if people want to play with it to experiment with it, it uninstalls nicely and cleanly.

Leo: Oh, that's good to know. That's really good to know. So you can always go back. GRC.com, that's Steve's site. That's where you'll find, of course, not only show notes, 16KB versions of the show, Elaine's written transcriptions so you can follow along, and even some great free programs for securing your system. Not to mention SpinRite, my favorite disk recovery and maintenance utility, SpinRite. It's from GRC.com. Well, Steve, this is a find.

Steve: Yup. I'm really, really glad we were able to turn out listeners on to it.

Leo: Really cool.

Steve: And we'll be back next week with Episode 130, that'll of course be a Q&A episode. Anyone who has questions or findings about SteadyState or any other comments or topics, please don't hesitate to go to GRC.com/feedback. Send your notes and thoughts to me, and we'll cover what we can of them next week.

Leo: And tell me what the name of that commercial program is that does the same thing.

It's just - same idea, you reboot the machine, it goes back to the pristine state. I can't remember the name. It's driving me crazy. Steve, thank you so much. Have a great week. And we'll be back next week with another great Security Now!.