Sandbox Limitations

Description: Having described "Sandboxie" and Virtual Machine sandboxing utilities in the past, Steve and Leo discuss the limitations of any sort of sandboxing for limiting the negative impacts of malware on a user's privacy and system's security.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-174.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-174-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 174 for December 11, 2008: Virtual Security. This show is brought to you by listeners like you and your contributions. We couldn't do it without you. Thanks so much.

It's time for Security Now! Episode 174. In a continuing series, continuing effort to keep you safe online and off, Steve Gibson is here. He's the security guru from GRC.com. Hi, Steve.

Steve Gibson: Hey, Leo. Great to be back with you. I have to say, when you say "continuing series," I get so much email from people who sort of append at the end, oh, and I hope you and Leo never stop doing this. Please, please, please, I look for this, my favorite podcast, or netcast. You know, just I look forward to it every week. Please, please, please don't ever stop. And that's germane, in fact, today, because we're actually recording this a week ago. We're having to get a couple episodes ahead in order so that we can provide content, Security Now! content to our listeners every single week throughout the holidays while you and your family are off in Paris.

Leo: "We're recording this a week ago" sounds like we've done some sort of science fiction thing.

Steve: I do watch - I watch "Sarah Connor Chronicles," of course. So we may very well have recorded this a week ago.

Leo: But we believe that we are actually recording this now for use in the future. You have a different point of view, ladies and gentlemen. You believe we've recorded this in the past for your listening enjoyment in the present. Man, this is a science fiction novel. What are we going to talk about today, Steve?

Steve: Well, our main topic isn't going to be extensive. I've got three interesting, contemporary security stories that occurred this week, which was actually a week ago last week in the future. So we'll discuss those. But I wanted to talk about I feel like I may have, two weeks ago on our Sandboxie episode, sort of maybe oversold what Sandboxie can do. We got a lot of email from people saying, oh, great, this is the only thing I need. I don't need to worry about antivirus. In fact, I think I even said that at some point. Like, oh, yeah, you don't need to worry about AV stuff because Sandboxie creates complete containment. And the same is true of virtual machines that also create containment. So I wanted to spend a little bit of time to walk myself back from that a little bit or, as Rachel Maddow says, "Talk me down," so to get a little bit more reality-based about the limitations of any kind of sandboxing thing and what bad stuff that gets into your computer can still do.

Leo: Well, and that's one thing I really like about you is that you have always been hard-headed. And as an engineer I think this is kind of an occupational hazard. You try to be very specific about what's so, and very honest, as opposed to somebody like me might get excited and jump up and down and say, ooh, it can do anything, anything, wash the car. So good. We'll get the reality-based facts here on Sandboxie and virtualization in general. All right, Steverino. Let's get the latest security news. Anything going on in the world out there?

Steve: Well, yeah. There were three really interesting security-related stories that I wanted to sort of extensively share with our listeners because they all bring home some of the topics that we've talked about. So I'm going to share each one, and then you and I will talk about what's essentially going on, what the story involves. This was the Boston Globe reported this. The headline would catch one's attention because it says "Sandwich loses nearly $50k to hacker."

Leo: What?

Steve: Well, Sandwich is a town in Massachusetts.

Leo: Ah.

Steve: So it was Sandwich, Massachusetts which loses nearly $50,000 to a hacker. And so the Boston Globe reported, they said, "The same type of data security breach that has menaced retail stores, restaurants, and other businesses has made its way into the Sandwich treasurer's office, where a hacker with possible international ties stole tens of thousands of dollars from town coffers in a complex computer-fraud scheme. Sandwich officials have warned their counterparts in surrounding towns of the computer breach. Police believe the hacker used a virus to attack Treasurer Craig Mayen's computer and implant a keylogger that monitored any keystrokes he entered." So this is the treasurer

of the town of Sandwich had a keylogger installed somehow on his machine.

"With technology similar to what is known as a 'sniffer,' a device that tracks computer information, the hacker was able to record Mayen's security code and password as he typed them, and used that information to make withdrawals from town bank accounts. The money was then transferred to four accounts - three in Florida and one in Georgia. Police Chief Michael J. Miller said yesterday that Mayen discovered the breach two weeks ago and notified police detectives. Investigators were able to determine that the scheme netted close to $50,000. Miller said yesterday that detectives will ask the state attorney general's office and the FBI for help in what he called a 'complex case.'" He said, "'That's the problem with tracking all this stuff, we don't have that ability,' the chief said. 'At this point, it's outside our realm of expertise.'

"Police have been working with the town's banks and a white-collar crime-fighting collaboration of law enforcement and bank security officials. Miller said police in Florida were able to question a man who opened one of the four accounts there as he was trying to make a withdrawal [from the account]. However, police do not believe the man is criminally involved in the scheme. The chief said the man in Florida, who was not identified, told authorities he answered an advertisement offering to pay him to open an account."

Leo: Oh, boy.

Steve: "The hacker would then move funds from Sandwich into the account, and the Florida man would then wire those funds through Western Union to St. Petersburg, Russia."

Leo: Wow.

Steve: "Miller would not say how much money was stolen from town coffers, but said it was less than [but approximately] $50,000. He said the culprits have been systematic in the account transfers in that each has been in amounts of less than $10,000, the threshold that banks use to notify FBI officials of significant monetary transfers. Mayen noticed the problem when he was conducting a bank transaction for the town and noticed a series of unauthorized withdrawals" - from under his own credentials, which had been stolen from them, he said - "beginning on [November] 4th under his security code. Gail Marcinkiewicz, a spokeswoman for the FBI, would not say yesterday whether her agency would assist the investigation." My guess is that they will.

"The FBI has jurisdiction to participate in such investigations, but any number of factors could determine whether the [agents actually get] involved. A spokeswoman for Attorney General Martha Coakley's office would not comment yesterday. The elaborate scheme is part of a larger underground computer fraud economy that has netted hundreds of billions of dollars through identity theft, credit card fraud, and other breaches, said Dean Turner, director of global intelligence network for Symantec. Miller downplayed reports that police are investigating whether the hacker has ties to Russian organized crime because of where the money was being sent. But Turner said that computer fraud is a booming industry in Russia and Eastern Europe, with organized crime rings offering all types of information and hacking equipment on the black market.

"'This is only a small slice of what's going on in the economy,' he said. The data breach

that occurred is similar to the type of scheme that attacked retailers such as TJX and BJ's Wholesale Club in one of the largest computer fraud cases in the country, Turner said. In this case, a hacker was able to implant a malicious code in the treasurer's computer. That could have been done in several ways, by email or through a website that was carrying the virus. From there, the hacker could have begun reading the keyboard strokes. Turner said hackers sell toolkits that can accomplish such fraud on the underground market. This is, what this really is,'" - what it really is. Oh, he says, "'...what this really is is a data breach, an ability to compromise information. In this case it's banking information.'"

Leo: Very interesting story. And I'm sure just one of many, some of which we'll never hear about.

Steve: Right. Well, and probably, based on how well organized this is, this is the sort of thing that we've talked about a number of times where it was probably a targeted attack.

Leo: Spear phishing.

Steve: Exactly. Spear phishing. So instead of just spewing email around, it seems very likely that the treasurer's office, if not the treasurer himself, was deliberately targeted, sent some email hoping he would click on it, using some known or maybe even unknown vulnerability. I mean, at this point certainly publicly they're not saying how this got into his system. It may well be, and it sounds like that the local police are not, at this point not equipped technically to go in and forensically figure out exactly what happened. Certainly the town treasurer has realized the kind of damage that can happen when his computer gets infected by something.

Leo: Right, right. A very interesting story. I guess you would think, if you were running this computer system for a town, you would have something like an Astaro Security Gateway maybe, or some sort of security filtering the mail.

Steve: Yeah. Again, we don't know what the vector was that brought this thing into his machine.

Leo: Seems likely to be mail, though; right?

Steve: That would be my guess. Given that it was targeted. Certainly you could probably get from the website of the town the email address for the treasurer. Or you could call up and pretend to be - do a little bit of social engineering, pretend to be somebody else and ask what the treasurer's email address is. Oh, I bumped into him, and he told me, but I didn't write it down. I thought I would remember it, but I forgot it, you know, what is it. And so then you start sending him things, hoping that he's going to act on it, and literally target him to install this thing. And then of course you're all set up, once you get control, with the backend money transfer system in order to get this stuff transferred through an intermediary so that it's not a direct connection. And then we know that unfortunately Western Union is how a lot of these funds get transferred out of the country.

Leo: Right. Yeah, I mean, figures, this is probably an operation, that they go through the websites of many, many municipalities, figuring especially small towns have less security. And once you've got the guy in Florida with the account set up, you can go through, you can have a number of checks go through. Doesn't have to be from Sandwich. Very interesting.

Steve: Well, I have another interesting story. This is the actual - I'm looking at the PDF from the United States Department of Justice, the DOJ, from the U.S. Attorney in the District of New Jersey who put out a report that I thought, again, touches on things we've talked about many times. This is from Newark, New Jersey.

"Law enforcement personnel in three states arrested four men this morning" - this is late November - "who were charged with engaging in an international conspiracy to deplete millions of dollars from U.S. victims' home equity lines of credit using personal information obtained through identity theft and unauthorized computer access," U.S. Attorney Christopher J. Christie announced. Today's arrests bring to eight the number of individuals charged to date in New Jersey with participation in [this single] scheme in which the defendants conspired to deplete available funds from home equity lines of credit, called HELOCs - just Home Equity Lines Of Credit...

Leo: Right, right, right.

Steve: "...belonging to identity theft victims, either by engineering fraudulent wire transfers or by gaining unauthorized access to the victims' online bank accounts. The four men arrested earlier today are," blah blah blah. They're scattered around the country - Los Angeles; Brooklyn, New York; Springfield, Illinois - who are expected to make initial appearances in federal courts in those towns.

"The defendants are part of a multinational identity theft ring that operates in the United States, the United Kingdom, Canada, China, Japan, Vietnam, and South Korea, among other places. The defendants and their co-conspirators have acquired identity information from thousands of victims and used that information to conduct numerous fraudulent schemes, including depleting their victims' home equity lines of credit accounts.

"The Complaints charge that co-conspirators have withdrawn more than $2.5 million from home equity lines of credit accounts belonging to innocent customers of banks and credit unions and have attempted to draw at least approximately four million more in ultimately unsuccessful transfers from those accounts.

"The Complaints charge that the defendants and their co-conspirators initiated the HELOC fraud by gaining access to confidential customer and account information used by customers of banks, credit unions, and credit card issuers to conduct finance transactions in the United States. This information included account holder names, addresses, dates of birth, account numbers, Social Security numbers, and account balances. Other fraud information frequently obtained by the co-conspirators during the course of the fraud included mothers' maiden names, security question answers, and online usernames, passwords, and other data used by banks and lending institutions to service and secure customer accounts.

"According to the Complaints, the defendants and their co-conspirators compromised confidential customer account information relating to several large and small banks,

credit unions, and credit issuers throughout the United States. The larger institutional victims identified in the Complaint include Citibank, JPMorganChase, Wachovia, Washington Mutual, Bank of America, among others. Dozens of smaller banks and credit unions have also been victimized, including the Navy Federal Credit Union, Pentagon Federal Credit Union, U.S. Senate Federal Credit Union, and State Department Federal Credit Union, and at least approximately 11 New Jersey-based financial institutions."

So here we have, I mean, like the raw information, all the facts associated with a major ring located throughout the whole United States. And bottom line, Leo, is this is about people using publicly available information to impersonate enough about a person in order to convince their lending institution that it's them. And oh, by the way, I want to withdraw money from my home equity line of credit and send it off in this direction.

Leo: Right, right.

Steve: We've talked - we've never really gone into detail about identity theft because it's a large and sort of amorphous topic. But one of the things that I take away from this is, and we sort of touched on this before, is do not use real, like your real information when someone says - gives you a form and says what's your mother's maiden name?

Leo: Right. Too easy to find out.

Steve: Yes, exactly. Come up with some other information. What's the name of your first pet? I mean, the Internet, it's often said that no information that ever goes onto the Internet ever leaves. And so, and for example, I was noting with interest the vetting process that people entering this next administration are going through and the questionnaire they've having to answer. They're having to say, have you ever written an email whose contents would embarrass you if it were made public? Well, okay.

Leo: Yeah.

Steve: Who among us have not?

Leo: Yeah.

Steve: You know? Like, okay, yesterday, and in fact maybe this morning. It's going to be a very empty White House, I think. I don't know how they're going to have anybody in there.

Leo: Well, they're asking for everything. It's amazing. They want everything. They want a complete...

Steve: Yeah, they really do. And so it's said that anything that goes on the 'Net never leaves the 'Net. And so similarly you could imagine the context in which you might have innocently answered a question about your first pet. And now we have Google that's able

to allow anyone to do deep research into people. I've also seen - someone gave me, like, a trial account for some of these online information-finding services. I was actually curious, I had lost touch with an ex-girlfriend, well, I should say a high school sweetheart, way way way. And I was able to find her to the home she had recently sold. And I called the owner of the home saying, hey, you know - and of course I'm very conscious of identity theft and security and things. And I didn't expect this person, I didn't even ask her what had happened to Terry, could she tell me who she sold the home to. But I explained that I was someone who knew her years ago, and I was hoping she was still there, and that's how I learned that she had sold the house.

But, I mean, you can literally - there is so much information available on the 'Net that I hope our listeners that are certainly people who care about this, and people who don't listen but who are friends of the people who listen, can get clued into this notion of absolutely not using valid information except when you absolutely have no choice. I mean, you can't lie about your Social Security number when you need to give it to the bank.

Leo: Or the government.

Steve: But you can certainly give Disney's turnstile your knuckle...

Leo: A knuckle. That's my favorite.

Steve: ...when it asks for your fingerprint.

Leo: Still my favorite letter we've ever gotten. Mr. G.

Steve: Hey, Leo.

Leo: Mr. G, you got any SpinRite email for us?

Steve: Yeah. I have agreed not to share Craig's last name because he said if - he's a Security Now! listener. And he said, if you share this, please keep my name confidential. So but his subject was "SpinRite Saved the Computer Outage Day." And he says, "Hello, Gibson Research Corp. Please forward to Steve Gibson, if possible. This is the first user testimonial I've ever sent for any software in my lifetime. I'm sure Steve is always very busy, but he does say that he loves to hear from users of SpinRite. SpinRite saved my power outage day."

So he says, "Dear Steve. Firstly, I would like to say thank you for all your hard work in both making the Internet a more secure place to explore and getting the word out to the world about security issues that are very important to us computer users. I've been following your site since 1999, when using Windows 98, before I was behind a router, and learned of ShieldsUP! to help me close my open ports and make my computer much more secure in many ways. A lot of the computer knowledge I have has come from reading your extensive information on your website. I've also been following Leo Laporte since The Screensavers and was happy to see the both of you collaborate on making

Security Now!. I've enjoyed listening to every episode since its inception. I still look forward to listening to it every week." So a great listener.

He says, "I finally bought SpinRite! I suppose, like most of our customers, we will all need to purchase SpinRite at some point due to a hard drive failure. Well, my time came to pass last month. I was working away at work, using my computer. There was a thunderstorm active that day, and the power went out for one or two seconds. When my PC was rebooting after the outage, I noticed it went into a repeating boot cycle. Every time, during the boot sequence, after the BIOS screen but before the Windows welcome, it would emit a clock beep and reboot. I thought I was a goner for sure. I called the support line for the PC, and they said the best they could do was to replace the drive.

"Well, even though I do back up, I only do so about once a month. And of course this happened in the last couple days of the month. So I thought, well, time to try SpinRite. I purchased and downloaded it and put it on a floppy. I powered off the PC, popped in the floppy, and started it up. Thankfully the BIOS was able to load SpinRite. I was worried that, depending on where the error was, it may not even load the floppy. I can't even remember which level I selected now, but I ran SpinRite. And after only maybe 30 to 40 minutes it was finished. It had found one damaged sector and stated that it had done its best to repair its data. So I thought, cool. Time to reboot and see what happens. Well, I was amazed to see it boot up like nothing had happened. Needless to say, I immediately backed up my data. I just wanted to let you know that you have another happy customer and a much more savvy computer user, thanks to your hard work. I will without hesitation recommend SpinRite to everyone who will listen. Thanks again."

Leo: That's great.

Steve: So thank you very much, Craig.

Leo: Always nice to hear those stories.

Steve: Yup.

Leo: So last, or it's actually two weeks ago now, we had the creator of Sandboxie on.

Steve: Yes.

Leo: And we talked a lot about how this sandboxing application could be used for security, to protect you. When applications run in Sandboxie, if you get a bad guy, some malware, whatever, it doesn't have access to the full machine. It's sandboxed. It's enclosed.

Steve: Right.

Leo: We also talked about virtual machines and how they can kind of do the same thing. A lot of people I know, in fact I do this myself, will instead of using Windows bareback, if you will, will run a virtual machine with VMware or some other program, and run that way. And that way, if we get infected, we just throw out the virtual machine and start over. But there are limits to what this can do.

Steve: Well, there are, exactly. And I feel like, as I was thinking about this, I thought, you know, I didn't want to give anyone the impression that Sandboxie or running things in a virtual machine was absolute protection against anything that malware can do because there is so much that malware can do.

Leo: Right.

Steve: For example, if you did - we heard earlier this example where a password logging program got installed on the treasurer's computer in Sandwich, Massachusetts. And that caused the loss of nearly $50,000 worth of funds transferred from accounts that he had access to, using his credentials. Well, that's a perfect example of something that Sandboxie would not have protected him from. Now, I'll say that with some caveat because, for example, Sandboxie would have not protected him until the sandbox was cleaned because, had he been using email - well, okay. Say that he installed himself - that this thing did use email as a vector of entry, as we hypothesize. Well, if he had a separate sandbox for it to contain his email client from his browser client, and if he were logging in to - we also don't know how he was logging in. But if he did have his email system sandboxed, and if it was clicking on a link that installed something is the way this keystroking logger got in, well, the keystroking logger would have been installed in the email's sandbox, so it would not have been able to log keystrokes in activities outside of the sandbox. So there he would have had isolation, so Sandboxie would have solved the problem.

If, however, if the keystroke logger had been installed in the web browser sandbox, and he used the web browser to log in, then until he cleaned the sandbox that keystroke logger would have been installed. I've got my Sandboxie sandbox set up so that it flushes the sandbox when no programs are running in it. So it just deletes the contents every time to prevent things from accumulating. And I ended up, after I talked two weeks ago, I talked about how I do - at that time I was using separate sandboxes for Eudora and for Firefox. And I ended up amalgamating them into a single sandbox because so often I am clicking links in email - I subscribe to a bunch of newsletters where they're trusted newsletters, like security newsletters, and they've got links to stories that are on the web. In fact, that's how I brought up those stories that I read earlier. So it's easier to have the email client and the browser sharing a sandbox because otherwise the email client is wanting to run another copy of the browser, another instance of the browser, in its own sandbox because things cannot get out of the sandbox.

So I decided, okay, look, let's just put email and my web browser together in the same sandbox. So in that scenario, because they are sharing a sandbox, if email were used as the vector to install the keystroke logger in this treasurer's office in Sandwich, Massachusetts, then he logged into the facility using the web browser, since they share the sandbox, they would share the keystroke logger, which would be a bad thing. On the other hand, if he were using some other sort of software outside the sandbox, then the keystroke logger would have been localized to the sandbox. Still not good, but it wouldn't

have created this compromise. So there's an example where something is being protected by the sandbox, but only within the constraints.

So notice that - my point is that the sandbox creates limits, and you would have the same sort of limits in any kind of a virtual machine environment where it would be installed on the virtual machine and not on your real machine, so activity outside of there would be protected, but not activity inside of there. And so, for example, if you were using all web browsing in that virtual machine where you now had a keystroke logger, you'd still be in trouble.

So I wanted to sort of further clarify the sorts of things that malware could still do. And so this notion of a password-stealer is a problem. Also things in the sandbox or in a virtual machine, they've got access to the network. It's because they are network-enabled applications that they're dangerous because bad stuff comes in from the outside. Well, that means they are able to initiate connections. A browser initiates connections out to the Internet. Email client initiates connections out to the Internet. Well, that means that programs running in the sandbox are Internet-permitted. Which means that, if malware got in there, notice that, unless you deliberately block areas of your system using Sandboxie - Sandboxie does permit you to, for example, blank out your whole My Documents tree, which is probably a good thing to do because your email client typically doesn't need access to that. It needs access to its own email repository. By poking a little pinhole through the sandbox so that that can be persistent while you flush the sandbox, you're not flushing all the email that you've received and replied. You want that to exist outside the Sandbox and persist longer than the life of the sandbox. But if you black out areas of your system, then nothing in the sandbox is able to access, for example, the whole My Documents tree where you may be having the bulk of the content that you're creating yourself on the system.

So it's certainly possible, if you had an Internet-enabled piece of malware, for it to read things in your system and send them out. You could have a spambot that you have unfortunately installed, doing everything it needs to, which is not what you want in the sandbox. Because if it came in through email, it has access to your email. We know that many spambots rifle through all of the email repository of the machine that they have access to and send out email pretending to be you, sending out something malicious to your friends. So that's a perfect, another perfect example of the kind of thing that no sandboxing environment can protect you from because everything it needs to do it has within the sandbox.

So it's very clear that this kind of sandboxing, while very useful, is not ultimate protection. And I did make a statement that I need to also pedal back from two weeks ago when I talked about the idea of testing, using a sandbox to test malicious software and drawing conclusions from the behavior of software in the sandbox and extrapolating that to outside the sandbox. The problem with really relying on that is that, as we know in the case of the Blue Pill work, it is difficult, but maybe not impossible, for software to detect that it has been sandboxed. And sufficiently clever malware - again, this is theoretical. But as we know from security, everything starts as a theory and ends up actually happening. Malware could deliberately behave itself if it knows it's running in a virtual machine or in a sandbox, believing that maybe it's being tested, it's being watched to see...

Leo: That's really interesting.

Steve: Yeah.

Leo: How can it detect it?

Steve: It could...

Leo: Does it have to use, like, Blue Pill kind of stuff or...

Steve: Yeah, I don't know off the top of my head how you could detect it, but...

Leo: I mean, a good VM, virtual machine or sandbox would hide the fact that you are inside a sandbox; right? It should look absolutely normal.

Steve: Yes. One thing off the top of my head, most VMs, for example, that are set up just to be used for containment testing, they're not very mature environments. They are a recently installed operating system that doesn't have the signs of having been used for years. There's not a whole bunch of documents in the My Documents tree. There aren't lots - there's not a whole, like, collection of programs installed in the system. So, for example, if software were to enumerate the uninstall list from the Control Panel, like here's the list of all the things that are available to be uninstalled, if there were not a bunch of them, it could be skeptical. Again, it would have to use some heuristics, some rules of thumb to judge that. But it could say, you know, this seems like a computer which has not been used awhile. I'm going to behave myself until I wake up in this machine, when it actually looks like it's been much more used. So that kind of thing.

Leo: Right, right, right.

Steve: And again, once then you trust the software, and you allow it to run on your native machine, it wakes up, looks at your list of removable software and goes, ah, now here's a thousand pieces of junk this poor sucker has loaded into his Windows machine. Now I believe I'm talking, I'm in the real Windows environment. And he can go to town.

Leo: Right, right. Well, and was it Blue Pill, or Red Pill, where it would test timing and...

Steve: Yes. I mean, it is...

Leo: That was clever.

Steve: In fact, there's been some evolution of this. Joanna said that the original Blue Pill 1.0 was undetectable. Well, now she's working on 2.0 because it turned out you could detect Blue Pill. You could tell that you were in the matrix, you were not actually in the real world.

Leo: This is the stuff I love the most in computer science. I love it.

Steve: It really is difficult to completely fool something. One of the things you could do is - and we talked about this then, for example. There is, scattered around the Internet, high-accuracy time references using NTP, Network Time Protocol, which systems are able to use to determine the time outside the computer. And so there are things you could do by comparing the passage of time inside and outside and look for differences because there are subtle differences in the timing of instructions because there is some virtualization overhead. That virtualization layer causes instructions to operate differently if it's present than if it's not.

Then the countervailing argument is okay, yes, but anything that the software running in the virtual environment does to detect that is in the virtual environment, so why can't you emulate it? And again, it's like, yes, in theory you can. But again, it's like the removal of spyware that we talked about last week. It's a cat-and-mouse game. And malware is upping the ante all the time to make it more difficult to root it out of the operating system, literally, you know, in the case of a rootkit. And similarly, software trying to detect if it's been Blue Pilled, if it's operating in the matrix and not in the real world, is being more and more clever. And so that requires that the virtualization environment become more and more clever in order to counteract it.

So what I wanted to explain, I wanted to really drive the point home that I love Sandboxie. I like it much better than a full-on VM.

Leo: Well, it's a lot simpler.

Steve: I use VMware. I've got it sitting here. I fire it up when I'm wanting to run multiple browsers and jump around. I like the feeling of knowing exactly what a virtual machine is. But I'm not running email in VMware, nor am I browsing in VMware because it's just - it's heavy. I fire it up for a purpose. It takes, you know, it commits a chunk of my system's memory permanently for the operating system, the copy Windows XP that I'm running in there, or different operating systems. So and in fact it's different OSes that is the big advantage with VMware because I'm able to host them on this single platform.

But I'm bullish on Sandboxie. I'm liking it a lot. I'm using it. It is lightweight. It does not tie up memory. I mean, it's always running and always providing containment for Firefox and my email client, Eudora. I mean, it's just pain-free. I'm 100 percent sold on it. But I wanted to make sure that I hadn't oversold it because I've given a bunch of examples here of things that could still be bad that are going on quite happily running in a sandbox, still not having behavior that you would want to have going on in your machine.

Leo: Well, fair enough. And I think if anybody says, ever, oh, I've got the silver bullet that will protect you from anything, that's suspect. There is - because there's so many ways, and these guys work so hard to figure out ways around that you've got to - it's constant vigilance, and you've got to use a variety of tools.

Steve: The cleanest thing to say about Sandboxie, which is my favorite solution for sandboxing, as I said, over using VMware, which I use for hosting different OSes, is that the cleanest thing, the way to put it is it prevents something from writing outside the

sandbox. It prevents what's in the sandbox from writing to your system. So if you sort of just keep that as the rule of thumb, it's like, okay, I know, I mean, that's a good thing. That's an important thing to prevent. But it's not everything. Because there's bad things that malware can do just by writing only within their own contained environment.

Leo: I want to ask you, in a second, where you would recommend Sandboxie, where you'd recommend a virtual machine, where you might recommend SteadyState. As I said, there are all these different tools. And some are better for some situations than others.

[Commercial break]

Leo: So Steven, so we now have in our toolbox kind of four related things; right? We've got Sandboxie; great. We've got virtual machines like VMware.

Steve: VMware, Virtual PC, Parallels.

Leo: Ton of them. Sun has one, I didn't realize. It's free. We have SteadyState, which we've talked about before, which is really cool technology that lets you kind of get back to where you were on a reboot. Each of these is a tool that seems to overlap a little bit. But they are, as you said, you would use Sandboxie in most cases?

Steve: Yeah. SteadyState is - it's very heavy-duty and heavyweight. I would say that's the right application for an untrusted environment. The real benefit for it is that there isn't anything that users can do to get around its encapsulation. The idea being that, for example, in a library where you've got public access terminals, you want to really lock them down. It's possible to lock down a PC without SteadyState using the Group Policy Editor. You can remove all kinds of privileges, I mean, it's freaky how customizable Windows really is. You can turn off, like, right-clicking; and you can turn off, I mean, like, all kinds of amazing little tweaks you can do to Windows if you really get in there and do that. The advantage with SteadyState is that it brings you that kind of group policy editor power just by clicking a few checkboxes. But more importantly, anything that someone does is being held in sort of in a file system buffer, very much like Sandboxie, where you're able to read, but any writes you create are cached so that you can read them back, but they're not actually modifying the hard drive. They're modifying a sandbox. So it's like Microsoft's sandboxing technology, which is bulletproof.

Sandboxie isn't made for that. Sandboxie assumes that, well, because it's just not its job. It assumes that you're using your machine, and you like your machine, you're not trying to abuse your own machine, because Sandboxie gives you the ability to control what it's doing. So its intention is different.

I would not use a system myself with SteadyState. And I've set up several for other people who are really concerned about security because, I mean, it doesn't slow it down. But the process of booting, when it boots up it has to flush the changes out. And it takes, I mean, it just - it feels much heavier when you're using SteadyState. So that's like the high end of the absolutely-allow-no-one-to-modify machine. It's from Microsoft, and it's free, and it works really well.

I would say next down from that is any of the VM solutions, whether it's Virtual PC, VMware, or Parallels, the main ones over on the Windows platform. And of course they're available now, because VMs are so widespread, on many different platforms. I can't see a reason for using one for just application containment because we really have that with Sandboxie. I see them as OS containment. That would make sense, as I said, for example, if I want to have a virtual machine running Vista or FreeBSD or Linux, that is, I want to cross-host operating systems. That's not something that Sandboxie can do, not ever intended to do. Sandboxie is an application sandbox, not an OS containment.

And so virtual machines, I think, really come into their own when you need to basically start with a pseudo-copy of an empty environment and install something, a whole operating system and upwards from there. And again, another reason that they're heavyweight is you have to have another licensed copy of the operating system. You can't use the same one. So that becomes burdensome. If you're using, for example, multiple copies of Windows, Microsoft wants to get license fees for all those.

So I'm back around then to Sandboxie, really feeling that, given that we understand its constraints - and notice that neither VMs, full-on virtual machines, nor SteadyState, none of them would prevent the kind of non-writing malware that we talked about. That is, they would, as long as you flush the state of your virtual machine, and you flush the state of the SteadyState environment, much as you flush the sandbox, you would turn those things into being transient. You'd get rid of them when you cleaned out that state. And so all three of these mechanisms have this notion of being able to reset the world to its prior state, which would remove anything that had crawled in. But while it had crawled in, before you had cleaned it, there are certainly bad things that can be done, but they can be done in every case.

So this is why I wanted to talk about sort of to generalize this notion of sandboxing, either with Sandboxie or VM or even SteadyState, doesn't completely protect you from every possible behavior of malware. But having said that, I'm back to Sandboxie because it is lightweight. It's running for me all the time. I don't have VMware running because I don't want to give it half a gig of RAM to run a copy of Windows XP. And with Sandboxie you have this lightweight, low-overhead, very nice solution.

Leo: Well, it's great to get the clarification. I love you for that. You're always impeccable in that regard. You don't want to overstate it. You want to be exactly accurate, and I appreciate that. And I have to say, once again, as I said last time when we talked about Sandboxie, I just wish it were available on the Mac because, unlike something like NoScript, which is a little more intrusive, that's something I would use all the time. I mean, that is - what a brilliant idea.

Steve: I am using it all the time. I should mention that I've exchanged an email with Ronen. I had a couple questions about whether it was filtering Windows shares access.

Leo: Oh, interesting.

Steve: Somebody in our newsgroup had said, hey, Steve, what if something just tried to open your C$, the default admin share, on localhost? And wouldn't that give it access? And good old Ronen, he's there ahead of him in this case. He understands that and blocks it.

Leo: Interesting.

Steve: And I also was writing to him about our topic for week after next, two weeks from now. We're going to talk about an interesting utility that was written four years ago by a Microsoft engineer called "DropMyRights."

Leo: Oh, yeah, I know about that. That's another one that our listeners often bring up as a good choice.

Steve: Right. And we're going to discuss it in great detail in two weeks. And it was in that context that I said, hey, Ronen, this is a cool thing. What about having that for Sandboxie? And he said, oh - anyway, we went back and forth a couple times. Turns out that Sandboxie is already doing a lot of that. It is dropping the rights in many different aspects to keep programs from being able to do bad things. But it's not doing as much as DropMyRights. Ronen, I told him that I was going to be talking about it; he says, oh, I think I'll add that.

Leo: Oh, that's so funny.

Steve: And I said that'd be good.

Leo: You know what I love, it's a real cat-and-mouse game between hackers who are smarter and smarter than ever, I mean, these guys really have an incentive now to really get into your machine, so they've gotten a lot smarter and a lot more clever. And the good guys, people like Ronen and you who are really - you guys have to use your brains, too. And it's just a fascinating intellectual exercise where, hmm, would they do this? And how would I stop that? It's point-counterpoint all the way down the line.

Steve: Well, and he did say in our initial email exchange that he had absolutely and definitely felt the effect at his end on us having told our listeners, all of our Security Now! listeners about Sandboxie and my being so pleased with the way it was working for me. So, and I'm glad because it means that a lot of listeners are now using this kind of protection to make their use of machines more safe.

Leo: It's interesting because, because Windows is the most attacked platform, in some ways it might be the most secure platform because there are the most defenses designed, the most patches, the most fixes, the most tools. You can use Windows very securely now. So I think that's fascinating, too.

Steve: Gotten a lot better in the last few years.

Leo: You bet, yeah. Steve Gibson, thank you so much. Next week a question-and-

answer session, so go right now to Security Now!'s website, GRC.com/feedback. Submit some questions. If there's something you'd like to know more about, we'd love to fill you in. Of course when you're there check out SpinRite, that's at GRC.com, the world's best...

Steve: Pays the bills at this end.

Leo: That's right, the world's best file and recovery maintenance utility file - hard drive maintenance and recovery utility. It also is just a tool that I use proactively, just to kind of keep an eye on things all the time. And we've found that to be very, very useful to SpinRite our drives before we put them in service. And he's got a lot of great free utilities there, too. You've heard about ShieldsUP!, Shoot The Messenger, DCOMbobulator, it goes on and on and on. Don't forget Wizmo. Love that Wizmo. And that's not even a security application. Well, it is now. You added a little bit of security to it.

Steve: Yeah, some WiFi stuff.

Leo: GRC.com. Steve, thanks so much. I guess - are we going to do a show on Christmas Day? I guess we are.

Steve: Absolutely. We're not missing any.

Leo: Steve never sleeps.

Steve: Christmas Day and New Year's, Leo.

Leo: All right. Well, get your shopping done. We'll talk to you Christmas Day on the next Security Now!. Thanks, Steve.

Steve: Thanks, Leo.