MojoPac

Description: Steve and Leo get deeply into the new MojoPac product from RingCube Technologies. After spending several days plumbing the depths of this intriguing new idea for installing secure and private Windows program and file installations onto transportable USB devices, Steve tells all about what he found and what he believes it means now and in the future.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-063.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-063-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 63 for October 26, 2006: MojoPac.

Security Now! is brought to you by Astaro, makers of the Astaro Security Gateway, on the web at www.astaro.com. And by Dell. For this week's specials, visit TWiT.tv/dell.

It's time to say hello to Steve Gibson and another great Security Now!. Hello, Steve, how are you?

Steve Gibson: Hey, Leo, great to be back.

Leo: Fall has hit. I don't know about Irvine, but Petaluma the leaves are starting to drop off the trees. It's really got a great fall feeling to it.

Steve: Well, you guys get a lot of rain up in Northern California, too.

Leo: We did. We got some rain, yeah. So, but it's been a little nippy, actually. So I think that's why. Warm during the days, in the 70s, but at night getting a little chilly. I don't know why I'm giving you the weather forecast.

Steve: I don't know why we're giving 100,000 listeners the weather forecast.

Leo: Yeah. That's one thing to give you the weather forecast. Maybe we should talk about security. What's up today?

Steve: Well, today we're going to talk about MojoPac.

Leo: MojoPac.

Steve: Last week I thought we were going to talk about MojoPac and U3 and something called moka5. But in the interim I've learned a lot about MojoPac. I did finally get a hold of the MojoPac people. Actually the parent company is a company called RingCube. I had a conference call with the CTO, their chief technology officer, to get all of my, you know, deep techie questions answered. The problem I had was that their website is all about features and benefits, you know, it's very sales and marketing. But, you know, as is always the case, I wanted to understand what they were actually doing, what was going on, you know, underneath. What was the technology? Was this virtual machine technology, you know, and how they'd implemented it, and to what level. Because what that – essentially everything that it can do flows from the way it does what it does, of course.

Leo: Yeah. And I think everybody's seen the hype, or at least a lot of people have, and kind of taken it on face value. And of course that's why we're counting on you to tell us what's really going on and if it really does what it says it does. We've heard some problems, too. I've gotten some emails from companies who say, you know, our licenses didn't work once it was installed on MojoPac, things like that, so.

Steve: Well, and I can address that because now I understand from – by understanding the underlying technology, I understand why they've had those problems.

Leo: Ah-ha.

Steve: And so as a result, and because U3 and moka5 and a couple other portable app solutions are so different, we're just going to talk about MojoPac today. This will be the MojoPac episode. And then but the other things are also neat in a different way, and so we'll talk about those in future episodes of Security Now!. In fact, I think, you know, like near-term future episodes.

Leo: Oh, good. Well, this kind of follows on what we just finished, which was our virtualization series. So this is kind of another kind. It's not really virtualization, but it's something else, something related.

Steve: Well, yes. So here's the story. MojoPac is a cool thing. I've downloaded it. I've been playing with it for a few days. And there's a lot of good about it. But what it's doing is difficult to do. Essentially, it's not virtual machine technology, as we've been talking about it, at all. What it, I mean, I don't want to say that it's rootkit technology because that has a negative connotation. But it's friendly rootkit technology.

Leo: Oh, interesting, huh.

Steve: What they're actually doing is, they are – they're installing a dynamic driver. So jumping ahead a little bit, you are a MojoPac user. You've got this USB device. And that can either be a hard disk drive or a solid state, you know, Flash ROM dongle. You stick it into an unsuspecting Windows XP machine that has never seen MojoPac before, has nothing Mojo-ish installed on it at the moment. And so what happens is the autostart.ini fires up, if it's enabled on that Windows machine, so – on that Windows XP machine. It's also important to say that this won't work on Windows 2000. This is an XP-only solution.

Leo: Okay.

Steve: So one issue is that, you know, power users may have disabled autostart; or, you know, other systems may have it disabled for one reason or another. So you may have to manually run the start.exe program on your dongle or your drive, if the hosting machine has autostart disabled. No big deal. But it's, you know, a little bit less automatic. In any event, when you run this start.exe, it essentially – it dynamically loads a kernel driver into the system which deeply hooks the Windows native API. We've talked about kernel hooks...

Leo: Those are words that scare me when you say that.

Steve: I know. And in fact I don't – the other word I don't want to use to describe MojoPac is "kludge" because kludge also has lots of negative...

Leo: Yeah.

Steve: ...negative connotations. But frankly, you know, a personal firewall, a third-party personal firewall is also a kludge because, you know, it's doing something to Windows that Windows was never designed to have done to it. And, you know, and that's why personal firewalls have caused problems for people. They've, you know, conflicted with other applications, things break, blah blah blah. You know, it's doing something deeply to Windows in the kernel that Windows was never designed to accommodate. Well, MojoPac is doing the same thing. And so in that same sense it's a kludge. But it's a kludge with benefits. I mean, it's...

Leo: It's a kludge with power.

Steve: It's a kludge that you might want to have.

Leo: Uh-huh.

Steve: You know, much like you want to have a personal firewall. So what happens is, when you install MojoPac, there's no virtualization stuff going on. Basically it reaches deeply into Windows and hooks the kernel, many of the kernel-level APIs...

Leo: See, already I don't – this is making me very nervous.

Steve: Well, and I'm going to read you, I mean, I'm going to flesh out this opinion which comes from the technology with some real-world examples of the consequences. So it makes

these low-level hooks. And this is the way...

Leo: You know, before we go too far, I don't think we've really described – have we described what it does from the user's point of view?

Steve: Ah, very good point. Let me back up, yeah.

Leo: We're talking about what it does from the technical point. But why would – why are people so excited about this?

Steve: You're right.

Leo: What does it do for the user?

Steve: Okay. So the experience I've had, which is why I started off saying this is a really cool thing, is I downloaded the MojoPac, the MojoPac exe. I installed it on a 512K dongle. Then I installed my favorite newsreader, Gravity; and I installed my favorite outlining tool, which is something called ThoughtManager Desktop, which I – because I love outlining, you know. I work from an outline every time I'm here in front of the microphone with you, Leo, because I, you know, going through all the points I want to remember about what I'm talking. So, and then I imported all of my working outlines. I got online, and I downloaded 3,000 newsgroup messages from the GRC news server, all in this 512K dongle.

Then I uninstalled – I shut down MojoPac and ejected the dongle, pulled it out, went over to another different Windows XP machine that had never seen any of this, stuck it in the USB port. MojoPac ran by itself, started up, brought me to a log-in dialogue, where I had to give it my password to log in. Then the normal desktop that I had been looking at on that Windows XP machine disappeared, was replaced by a brand new Windows desktop that looked just like what I had when I removed the dongle from the first machine. And there were in the – you know, the standard Windows-looking Start button, I mean, it is the Windows Start button and programs. There was my newsreader, Gravity, and my outlining ThoughtManager, both running, I mean, able to run. I brought them up. There were all my postings.

And so what it creates, basically it allows you, through all this work that these guys have done, to sort of have a portable Windows install of your own that can run off of any USB 2.0 device. So, for example, I mean, a cell phone that's got an additional memory card installed, or your iPod, or, you know, anything that is USB 2.0, you're able to install MojoPac and basically build yourself your own portable Windows environment that is not just your data, but also your applications.

Leo: That's impressive.

Steve: Well, and that's the big difference. Because, you know, certainly people have been able to, you know, synchronize their data and, like, move PowerPoint files or...

Leo: Briefcase did that. I mean, that's no big deal.

Steve: Exactly. So the real difference here is you're able to install applications. Well, the way they've pulled this off – and it's important to note also, these are any applications. In a couple of weeks we'll be talking about U3, which is sort of like this, but U3 takes a very different approach of creating an environment where applications have to be aware that they're running from a solid-state device. The MojoPac guys have basically, by deeply hooking the Windows kernel, they have – they're basically simulating a standard Windows environment on a USB device.

Leo: Wow.

Steve: So the applications are none the wiser. Now, there's some caveats to that because, since they're not performing full virtualization, the applications may notice that they've been moved to a different machine.

Leo: Ah.

Steve: Now, again, this is the kind of thing that can probably be, and some cases definitely will be, fixed in the future. For example, users immediately noticed that the retail version of Office would, when they moved it to a foreign machine – they had installed Office apps on their MojoPac USB device. When they moved it to another machine, it said, okay, you need to activate me. So Office deactivated because it...

Leo: Right, right.

Steve: ...saw that it had moved to a different platform. In a true virtual machine environment, as we know, the app doesn't know, can't know that it's on a different machine because the entire environment has been virtualized. Here, MojoPac is doing what it needs to to make the applications run. However, Mike the CTO guy that I asked this question of said in the next release of MojoPac they will deal with making Office function universally.

Leo: Wow, wow, wow.

Steve: But now, but this is sort of the – the way I want to characterize this, I want to characterize it carefully for people. My sense is that it's a quirky system because what these guys are trying to do is difficult. In the same way that the very first personal firewalls were much more quirky then than they are now.

Leo: Well, and I even think of things like DESQ and application switchers, where you're really trying to get into the hooks of the operating system and change how it behaves...

Steve: Yes.

Leo: ...you're just really taking some big chances.

Steve: Well, so let me give you some examples. For example, from their own knowledge base, they cannot install on a system where there are multiple – where you have a multiboot

operating system that's booting from drives other than C. You know that it is possible, for example, to have C, D, and E partitions or drive, and have the OS actually installed on D or E or a non-C: drive under Windows. MojoPac can't handle that. Another example is host machine screensaver and power management, they say that some failures have been observed when the host machine's screensaver or power management options become active. Under printer drivers, kernel...

Leo: Oh, that's kind of a problem.

Steve: Oh, no. Just wait, Leo. Kernel, you know – sometimes, they're saying, kernel mode printer drivers will fail installation in the guest, that is, in the MojoPac guest. This includes programs that install their own virtual printer drivers, such as Adobe Acrobat.

Leo: Okay, so that doesn't work.

Steve: But, I mean, it's important to know that Acrobat Reader does. It's just the – it's the Acrobat distiller, you know, Acrobat pseudo-printer that can't. But then they say this limitation will be addressed in a future version. It says that certain...

Leo: I bet they have a pretty long list of limitations to be addressed in future versions.

Steve: Well, yes. Let me go a little bit further, here, just to sort of flesh out this notion. This is under COM+ applications. Certain applications that require COM+ may behave strangely or malfunction. Under the Recycle Bin, on some PCs deleted folders may not appear in the guest after file/folder deletion. However, there may be items to empty in there. My own experience, I like to have AutoArrange turned on on my desktop. And it's just not sticky. I've never – I keep turning it on as I move MojoPac from machine to machine, and it doesn't stay. Neither do the icon positions. Because I like to sort of organize where things are, and it sort of forgets where they were previously.

Under Word and Excel, they say that Excel docs containing a font symbol that was created on XP Pro Service pack 2 showed the symbol as an unrecognizable value and opened on the guest plugged into host without MS Excel installed. They say you may see problems with OLE when opening docs with Office. Windows Media Player: Users are advised not to install Windows Media Player 11 within MojoPac, as it will lead to unpredictable behavior, and recovery to the previous stable state may not be possible. Under reboots by third-party applications: Reboots by third-party applications may not always work. The reboot is usually requested during the application install. I mean, and this goes on and on and on.

Games, for example, one of the cool things you can imagine would be like a World of Warcraft addict wants to carry his whole World of Warcraft environment around with him so that he can go to a foreign machine, plug in, and just be up and running. Except that it says: Certain games, such as World of Warcraft, exhibit offset mouse movement at the end of install. In other words, clicking on a control, a Windows control, will not trigger the desired action. The user should move the mouse around the control to find the amount of offset from the mouse's visible and actual position. The mouse can...

Leo: [Laughing].

Steve: I know, I know. I'm reading this going, oh, my goodness. The mouse can then be

moved to the offset location in order to activate the control. Note: This behavior does not occur when the user plays the game.

Leo: Oh.

Steve: So something about the game is causing the mouse's visible location and its effective location to be skewed. And so they say, well, sort of, you know, hover over things and see when they light up to figure out where the mouse actually is. So, I mean, and there's, like, a lot of these things. So, and so this is why I have to kind of characterize this as a kludge. But I don't want to put people off of it because, for most things, I think it really works. I mean, I don't actually have a need to move, you know, my newsreader and all of my newsgroups around and to do this kind of thing. But I'm sure there are people who have this kind of need, and it really does work.

Now, what happens is, when you are looking at the Mojo desktop, there's a bar at the top, the MojoBar, that is unfortunately about the ugliest thing I have ever seen. I right-clicked on it, and there was a little popup saying "return to default skin." So it was like, oh, great, maybe I could, like, fix this. Well, this is actually reminiscent of ZoneAlarm. Remember that day-glo orange...

Leo: Oooh, yeah.

Steve: ...that ZoneAlarm, those ZoneAlarm guys use? Well, I mean, I loved the firewall back in the beginning. But I used to tease them all the time about how horrible, you know, the horrible colors they had chosen for the UI. Well, the good news is, apparently this MojoBar, their own toolbar, is skinnable. And I'm sure people are already hard at work in replacing the default skin, which is just godawful looking. I mean, it just ruins the look of the rest of your system.

But, you know, it does work. And it allows you to instantly, with a single click, to switch back and forth between your Mojo-ized desktop and the desktop on the host. When you're looking at the host view, you can see the Mojo drive, and you're able to copy any things that you want to to it. Sort of from the host side, it looks just like a regular drive. They also provide a cool synchronization utility that allows you and offers to sort of, like, move your whole documents and setting tree over so that all of your settings and your whole My Documents group are moved over. So that's very – it makes it very easy to synchronize and to set things up over there.

One of the things you cannot do is – and this is one of the most often requested things that they are never going to address – is you cannot simply move preinstalled applications from your host machine into the Mojo environment. And this is deliberate on their part. Also it's very difficult to do, as we know, because it's very difficult to move an already installed app to, you know, anywhere, because apps can do so much to the system when they install themselves. But these guys recognize that they have, in creating this notion of mobile applications, they've really turned the license, the software licensing model, upside down, I mean, on its head. Because if you look at the EULAs, the End User License Agreements in virtually anything you install, it says this is for use on one single computer.

Now, I talked to them about this explicitly. And they said, well, you know, actually we looked at a lot of EULAs. Many of them say on two – you can do two installs because they want to be laptop friendly. They want to allow people to install on their main workstation and also on a laptop. I'm going to give them the benefit of the doubt on that. The EULAs I have seen tend to say only use this on one machine. So inherently your – this is a multi-machine install. You're installing the application that the EULA says you can only run in one location; you're installing it on an inherently portable device. You know, my feeling is you make one of the installation of the app. You are carrying it around. You're the only one using it. I would say, even though it

might be outside the letter of what the EULA was written to say, the EULA wasn't written with Mojo in mind. So, you know, I wouldn't consider that a big breech of the publisher's license.

However, this is why the MojoPac guys want to be very clear that, when you install MojoPac from the start, basically you start off with what looks like an empty Windows system. It uses Windows profiles. Basically it creates a mobile user profile on the MojoPac device. And you end up looking at, you know, a virgin Windows desktop with a Start button and nothing in the programs group. And you must then manually reinstall any things from scratch that you want to have on your MojoPac and be portable. The MojoPac guys feel that this deals with the upside-down nature of portable licensing in a good way because basically they're saying users are being given the responsibility of installing or reinstalling existing applications if they want them to be portable, rather than, for example, MojoPac just cloning them somehow into this portable device, which they're explicitly not willing to do.

So, you know, that's sort of the gist of this thing. It's a small download. It's only about a 9MB download. It's not currently digitally signed, which is a point I brought up to them; and they said, yes, we know that, we're going to fix that. Because of course now Windows and certainly Internet Explorer is becoming increasingly reactionary to the idea of not having, you know, of users running non-signed things that they've just downloaded from the Internet. You get all kinds of unknown publishers and are you really sure you want to do this kinds of messages. The release price was basically half-price, $24.99. It is going up to $49.99, that is to say, $50, in just three weeks. I think that's a mistake. On Thursday, exactly three weeks from today, Leo, Thursday, November 16, the registered price of MojoPac doubles up to $50.

Leo: Ah.

Steve: I really think they should, given that they've still got so many little bits of debris to work out, my advice would be, what's the hurry, you know, extend this special offer time another couple months, especially since they had a bunch of problems when they came out of the gate, you know, taking it out of beta. I really think this is a much too narrow Window. I guess it's really only been about a one-month Window before they jump the price up. As I understand it, they're venture financed, so they shouldn't have cash-flow problems.

And I really, I mean, I would encourage people to play with this. The way it works without registration is you get 30 days of use or 200 boots. And they doubled that number of boots recently because people were running dry well before their 30 days were up. They only had 100 boots before. That is actually 100 stick the MojoPacs in a computer is what's called a boot. And so, you know, I've already used up 15 of mine just moving it around in a couple days, you know, playing with it. So if people think this might be something they're interested in messing with, you've got three weeks before the price doubles.

The other good news is, as you know, I'm very sensitive to things impacting my system. You know, I didn't like installing, you know, VMware on test machines or, like, messing with Virtual PC and these other things because, I mean, these, like, these whacked your machine. MojoPac doesn't. As far as I can see, it makes zero change to the machine on which you download their exe and where you install MojoPac. And that's all part of their philosophy. When you shut down MojoPac and remove it from a machine, their dynamic device driver unloads the machine, that host where you were temp- that you were temporarily visiting and basically using its resources, its network and processing and screen and other resources. It ends up not knowing anything has happened. And that's the magic of their kernel-level hooks. The apps running in MojoPac see a C drive, but the C drive is the actual MojoPac device remapped to C. And the actual host C drive is not available. It is inaccessible. So there's no changes being made to the registry. There's no debris left behind, no browser settings, no trail of URLs you visited. Nothing changes on the host.

And so from a security standpoint, you know, this is one of the main advantages that they were

going for. And this is unique among these other solutions. We know, for example, there's Sandboxie; and there are, you know, full robust VM solutions. But any VM solution is inherently going to seriously sit on the machine you install it on. So in that sense, MojoPac is very lightweight. It's, I mean, and I have to say, I mean, I like it. I would encourage people not to be put off by, you know, their list of knowledge base, yes, we know we have these problems. I mean, I found some myself. Right-clicking on Network Neighborhood, which is now renamed My Network Places under XP, nothing comes up. I right-click and do Properties; I can't get properties. I thought, okay, you know, what's going on? So I clicked the MojoBar at the top, instantly switched back to the host, right-clicked on My – I forgot what it's called now. Network Neighborhood or My Network Things. And the dialogue...

Leo: My Network Things is good. I like that. I'm going to recommend that for Vista, yeah.

Steve: And, you know, and everything was as I remembered it. Back over to Mojo, and that just doesn't work. So it was like, okay, add that to the list. So the point is, what they're doing is something Windows was never designed to have done to it. And frankly, this is such a cool idea. As long as we sort of tolerate the question of mobile licenses, which is still a little bit up in the air, in my opinion, but the idea is so cool, you can imagine that in some future version of Windows that, you know, this won't be something Windows fights. It'll be something Microsoft acquires, much as Microsoft finally added a personal firewall to XP, you know, several years after everybody else had gotten bloodied on the battlefield developing the technology. I could easily imagine that this kind of portable application stuff is so cool that it ends up ultimately, you know, generations from now, appearing in Windows. But it's available today.

Leo: I might just point out that Apple's had this for about ten years. But okay.

Steve: Thank you, Leo.

Leo: And actually it's not – that's really not fair. In fact, it may even exist for Windows. But Apple networking could be set up so that, no matter where you are on the network, when you log into your network, it's your desktop, your preferences, your applications.

Steve: Oh, cool. And, well, now, Windows has that, too. It's called a roaming profile.

Leo: Roaming profile, right.

Steve: Yes, and so...

Leo: This is not quite that, but this is – allows you to do kind of a roaming profile, right?

Steve: Well, this is way more than that because the roaming profile doesn't provide you any of the encapsulation that MojoPac does. I mean, remember, you could literally install Firefox – they've got problems with IE7 right now.

Leo: I may be wrong, but I think the Apple one does do that. But I may be wrong on that.

Steve: Provides real security encapsulation?

Leo: Yeah, basically everything's all kind of packaged up.

Steve: Well, okay. But I guess...

Leo: I don't know. That's a good question. I don't know.

Steve: I'm sure there's no access to the host. Because, you know...

Leo: Oh, I see what you're saying.

Steve: Yes.

Leo: No, I think you probably would access the host. I think it's probably all living on the host.

Steve: Yes. And so that's my point is that what Apple has done...

Leo: I see. You're taking it with you. It's completely portable. Right.

Steve: Well, but not only portable. And again, I want to make sure we make this point. It's encapsulated. That is to say, when you install your MojoPac device into the machine, it brings up the MojoPac desktop into which you log in, and you have no access to the normal host's resources. You cannot get to the hard drive. You cannot get to – you're able to access removable media. You can see the host's CD-ROM and DVD and other USB devices. But basically you're only able to see those things which the MojoPac guys allow you to see.

It's also important to note that you do have to be logged in as an admin user, a full-strength user, on the host. They have provisions which they will be making available to universities because you can imagine in a university setting, all the university students could have MojoPac, you know, in dongles around their neck. And they go to bolted-down, limited-user XP systems, stick in their dongle, and now they've got access to, you know, their own portable environment. And so there is a way that MojoPac can run as an admin user on top of a limited user host, but that's not the normal retail version. That's not what people can buy right now. Right now you do – the host that you stick your MojoPac into needs to be running as an admin in order for MojoPac to install itself and make itself go. Because, again, it's installing a dynamic, very low level kernel driver in order to perform all of this – all these modifications to Windows.

It's also worth noting that there are sort of two profiles that have sort of surfaced for MojoPac users. The people at RingCube who did MojoPac all literally use MojoPac as their single environment. They use small USB 2.0 hard drives, as opposed to solid-state drives. And they have installed all of the applications they use, I mean, basically their entire PC is installed in a MojoPac drive. And so what they have when they come to work is literally an empty Windows XP machine. It's just – it got a generic install. It's sitting there with nothing on it. They come to work in the morning, plug their drive in, bang, they're looking at their desktop, exactly as they left it at home, because they've done the same thing at home. They've got a generic Windows

XP install at home. And when they come back from work they plug their drive in, and their whole environment is portable and has moved with them, including all the applications that they have installed. So you have sort of this high-end whole environment portability user, where, for example, the relatively limited size of a USB dongle, which is, you know, practically, you know, 4-gig, maybe 8-gig today, and the somewhat lower performance of a Flash ROM device may not be enough for that kind of a user. So you use a small, lightweight, you know, portable USB drive.

Then you've got somebody like I was pretending to be a couple days ago where, I mean, I really wanted something in my pocket or on my keychain. And that's entirely practical. There have been some postings on the 'Net about slow performance problems with MojoPac. I don't see that at all. As far as I could see, I mean, I was using a good Sandisk, 512K, high-speed USB device. But I downloaded 3,500 newsgroup messages just as fast as I would have on a regular PC. They claim about a 5 percent overhead of their system, which is very low for this kind of work. But it's really not doing much. It's just filtering at the kernel API in order to sort of mutate the Windows environment in order to MojoPac-ize the host machine, to hide the hard drive, to allow you to get access to the networking layers and so forth, and basically to provide this MojoPac desktop.

Another example of sort of the kludgeness of this is, if a personal firewall pops up a message, it pops up on the underlying host desktop, and you can't see it. So to get around this, the MojoPac guys are watching for anything popping up on the desktop underneath, and then will provide you with a notice that something has popped up on the host desktop, which requires you to click the MojoBar, flip over to the host, and see what's going on. One of the other errata is that if a personal firewall blocks something that you're doing in the Mojo environment, you may need to go back to the host and to permit the application, which is running on Mojo, to go through.

I mean, again, these are consequences of the fact that Windows was never designed to have this done. It's a testament, the fact that these guys are able to do it at all is a testament to their courage and fortitude and, you know, the fact that they had a really cool idea, which I'm sure is going to be evolving and improving and getting better over time as they work out all of these sorts of, you know, dust and debris, much as I remember personal firewalls being in the beginning, and now they're much more solid.

So again, I don't want to put people off. Neither do I want to oversell this. And the reason I think that this evaluation period is critical is people ought to give it a try. It is, you know, everyone who sees it says, whoa, this is so cool. I mean, and I feel that way, too. If I were – if my life were such that I was ever away from here, and I wanted to carry an executable Windows environment with me, and I knew that there would be host – there would be available admin-privileged Windows XP machines wherever I was going to need to do something, and I'm carrying all my data, I mean, it is really a cool solution. And it works, but it can be quirky for specific things. So you'd want to make sure, for example, if you were someone who needed to use Adobe Acrobat's PDF creation capabilities, that's just not working under MojoPac today because it's something that you can imagine they will probably get around to dealing with at some point. Thus my sense is that this is going to keep getting better and better.

Also, relative to licensing, you've got this 30 days or 200 boots, and then you've got to buy it. And don't forget, from the time people are hearing this, there's a three-week window during which buying it is $24.99 versus twice the price at $49.99. So keep that in mind, too. Once you have bought it, there is the ability to migrate your MojoPac from one device to another. They only run on USB 2.0 because USB 2.0's spec requires a unique serial number on every device. So they're locking their license to it.

When you download this 9MB MojoPac install and do your install, you create an account over on the MojoPac site, a username and password on the MojoPac site. And you use that same username and password in order to subsequently access your device, although you're able to change the password. And in fact I think they prompt you to change the password the very first

time you use this. So you've installed one instance of MojoPac on one device. If you outgrow that, or you decide you want to try a faster USB, or you want to move over to a hard drive or do whatever you want to, they provide the facility for deregistering the current MojoPac install and copying it over to another device and reregistering it there. So you are able to migrate your purchased MojoPac to USB devices virtually unlimited. I think there actually is a high limit because they do want to prevent fraud, you know, some style of fraud from occurring. But basically it would never be something that would impede MojoPac's users.

Leo: I think, though, I mean, it's something that really should be done at the operating system level. It just doesn't seem like an independent software vendor has a chance of making this thing work. I mean, Microsoft changes one thing, the whole thing collapses.

Steve: Well, that level of kernel API is pretty stable. I asked them about Vista because of course Vista, as we know, is very hostile to anyone mucking...

Leo: Right.

Steve: ...around down in its innards. And they claim that they have it running on I'm sure the 32-bit beta of Vista.

Leo: Interesting.

Steve: I think it's running under RC2. And again, the kernel API is a well-documented, well-structured, well-understood API.

Leo: All right. So this is an accepted thing to do.

Steve: Yes. Well, it's, you know, I don't know what they're going to do under the 64-bit version of Vista. In the same way that McAfee and Symantec are frozen out from going in and mucking around, I have to imagine that MojoPac would be similarly prohibited until, as Microsoft has said, with Service Pack 1 of Vista, the 64-bit Vista, then they will provide an API. But that's apparently only a monitoring API. That's probably enough for Symantec and McAfee. It may not be enough. So it may be, I mean, this is, again, this is another example of why, reluctant as I am to call this a kludge, that's the word for it because they just may never be able to do this under the 64-bit version of Vista because Vista won't let you go in and do this. Because again, as I said, it's rootkit-ish behavior, and Vista 64-bit is specifically anti-rootkit.

Leo: Right.

Steve: But Leo, really, I mean, you ought to try it. I'm encouraging people, with all of these caveats I've thrown out.

Leo: Oh, I'm so reluctant to try it, Steve. How do you get this thing off of your system? Do you think it uninstalls cleanly?

Steve: No, no, it's never on your system.

Leo: It's never on your system.

Steve: No, that's what's so nice, is you download the 9 megs, you give it a USB device. Now, they suggest...

Leo: So wait a minute. It only modifies your system in memory on the fly? It never changes your operating system?

Steve: Correct. It doesn't change the OS you originally install it – you install the MojoPac onto, nor does it ever change anything...

Leo: Okay.

Steve: ...about a guest operating system. I mean, that part I'm really clear about.

Leo: All right.

Steve: And it's why, again, you know, I know I've been – I've thrown up all these caveats. But it actually does work.

Leo: If it doesn't modify my system, well, of course I'll try it. Why not?

Steve: Yeah. Well, and as I said, you know, installing VMware is a horrifying thing. I mean, it creates virtual adapters. It's got stuff running constantly in the background. It's got services running. It's all this stuff. You know, VMware doesn't – MojoPac does not do this. Nothing on the system where I originally installed it, I mean, nothing was even installed there. The little 9-meg installer just found my USB device, asked me choose which one I wanted to install it to, and it moved itself over there. Nothing changed on my host system. Then, when you install and you plug it into guest systems, it just dynamically loads this driver in RAM. Nothing is written to the hard drive. Your MojoView has no access to the registry, to the hard drive, or anything, so that anything you do is encapsulated. And there's nothing to uninstall because it's never installed. I mean, it is – again, I think these guys are in, you know, the first phase of a very cool thing, and that a year from now, two years from now, we're going to look back at this, you know, at Episode 63 of Security Now! and go, well, you know, we were right. This thing had all kinds of wacky behavior, but they nailed it down.

Leo: I'm going to make you a deal. They're going to say, Steve was right, Leo was full of it. Because I don't think this is ever going to happen. And I think really, if it does, it should happen at the operating system level. But all right. If you think you...

Steve: No, no. Now, Leo, I'm not saying I disagree with you, except we don't have it available at the operating system level.

Leo: Well, Microsoft's not doing it. Yeah, Microsoft's not doing it.

Steve: And it's going to take them generations. You know, Vista is already done. So it's not going to be in Vista. This is not something I could see them adding in a service pack. So it's going to have to be in Wista. Or, you know...

Leo: Mista.

Steve: ...whatever comes after Vista.

Leo: Sista.

Steve: And, you know, and that's going to be a long time.

Leo: Right.

Steve: So, you know, no one should hold out hope for this happening sooner.

Leo: No, I understand that. I understand that.

Steve: But I agree with you. I mean, in the same way that I think a personal firewall should be in the OS because, you know, that's the right place for it. You know, this notion of application portability, installing normal hard disk-targeted apps in a portable device, this is a cool thing. When people see this, this is cool. I mean, and the MojoPac guys have done, as I said, they had a lot of guts, and they've tackled something which is fundamentally hostile to Windows, but they're making it work.

And so again, because it's a small download, you get 30 days to play with it, it won't screw up your system, it won't modify any guest systems, and it does allow you to have – to take normal, regular, non-special Windows applications and run them on a portable device, and that it's really portable, and it creates privacy and security encapsulation for what you're doing on the MojoPac. As I think I heard them say when we were talking on the phone, you know, what happens in MojoPac stays in MojoPac. I mean, it is very cool. It's just it was a huge challenge to do this. I...

Leo: I give them props as hackers, absolutely. I give them props.

Steve: Absolutely. I salute them and tip my hat. I mean, this is a very valuable thing that – you know, and I'm feeling, again, 50 bucks seems like a lot of money. On the other hand, I'm charging 89 for my software, so who am I to talk? But it does allow you to move around your purchased MojoPac from device to device. They suggest – and this is all in the ReadMe file, that I do encourage people to read – they suggest, for example, that if you can, you reformat your dongle to NTFS rather than the default, which will be a FAT or FAT 32 file system. Obviously people who are using an iPod can't. They're not able to reformat. They're going to have to leave it in its default FAT format because they still want to be able to use their iPod, you know, on a Mac, I guess, or on, you know, in the way they normally do. So they're not able to change that to NTFS. But if you did have a standalone drive or a USB device which you're able to use with NTFS, they're just saying security is better and it is faster than FAT. Oh, and I forgot to mention that something that they did broke compatibility with TrueCrypt. I was concerned...

Leo: Oh, boy. Now I've had it.

Steve: No, slow down, slow down. I was concerned about that, so I asked them. They recognize they broke it. They've come up with a temporary workaround that allows TrueCrypt to be used. And the next release will be completely TrueCrypt friendly. So our favorite ultra-robust security tool can also be used with MojoPac in order to allow a TrueCrypt volume to be carried and to have – and where TrueCrypt is running on MojoPac, no longer do you need to install TrueCrypt on the target system. So that's even better than running TrueCrypt by itself. Because if you had TrueCrypted a dongle or a drive, you would need to install TrueCrypt on the host machine in order to then have portable access. Here, TrueCrypt is running in MojoPac, giving you access to your TrueCrypt partition or directories. So, I mean, in some sense it's even better than TrueCrypt without MojoPac. And these, I mean, they are committed to the issue of security and privacy, so they're going to make it work even better than it does now. And it does work now, although you need to do some workaround.

Leo: You might, I mean, if all you really need is email and browsing, there are USB versions of Firefox and of Thunderbird and so forth that you can carry on a USB key, keeps all your stuff on the key. It doesn't have the same kind of encapsulation you're talking about. But you can do that.

Steve: Well, that's absolutely true. And in fact, U3, which we'll be talking about in the future, is a specific platform for running things from Flash. There are, you know, the real advantage of MojoPac is encapsulation because Firefox won't give you this kind of robust encapsulation. If you did get something, a virus or something, in Firefox running from a dongle, it would still have access to your C drive. And so again, I mean, there are real benefits to what the MojoPac guys have done that, as far as I know, are unique. It's true that if you were carrying a virtual machine around in your dongle, and you knew that you had VMware or Parallels installed in any host machine, you could simply launch your VM and then operate. But that requires a serious hit to the hosting platform. MojoPac doesn't hit the hosting platform at all.

Leo: Is Flash fast enough to do this? I mean, you're running stuff, not off the hard drive but off the Flash.

Steve: Well, you are. But the way Windows operates – first of all, Flash reads at about twice the speed that it writes. Another concern is that Flash has a write limit. The actual chemical technology of the non-volatility of a Flash has a maximum of about 100,000 write cycles. So, for example, people who arrange, like, Flash-booting Linux systems, in fact I have myself a Flash-booting FreeBSD system that I built, I had to go to some lengths to not have a swapping partition on the Flash. And in fact, to make sure that I was mounting my Flash partitions in read-only mode, so that the system would be logging to RAM and to Flash, because you never want a situation where by default you're writing often and hard to your Flash because it will end-of-life that device very quickly. Mark Thompson actually did some experiments where he burned out a Flash in a couple of days...

Leo: Wow.

Steve: ...just by booting a standard Windows system. And Windows just thrashed the thing and killed it. And...

Leo: Well, the good news is now that Flash is at least fairly cheap. So, you know, you might use it for six months and have to buy a new one.

Steve: Well, and I asked this question of the MojoPac guys. They've been using MojoPac for six months, many of them on Flash devices. And naturally they've been testing it and pounding on it and using it like crazy. Not a single one of theirs has ever died.

Leo: Ah, that's good.

Steve: I would encourage people not to use bargain basement, you know, cash register, oh, here's a $15, you know, half-a-gig Flash that you can get at the checkout stand. But by all means stay with, you know, Lexar or Sandisk or a high-end, good brand Flash.

Leo: Is there really a difference?

Steve: I really think there is, yes.

Leo: Hmm, interesting.

Steve: I mean, certainly in performance, too, because in order to get accelerated performance, what they're doing is they're writing in parallel to many more Flash devices inside in order to get multiples of write speed. And there's also something called "write leveling," which expensive Flash has and cheapo Flash doesn't. What write leveling does is it actually distributes the writes so that, even though you appear to be writing to the same logical location in the Flash, it's actually the Flash itself is writing, and it's doing sort of the equivalent of sector swapping on a hard drive. It's actually writing to other physical areas, which are then read back from that area, sort of in a content-addressable scenario. So the idea is it means that if you were only using part of your Flash and, like, recording pictures, deleting them, recording them, deleting them, recording them, deleting them, and like never filling up your Flash, on a normal FAT file system that would end up burning out the front of the file system...

Leo: Oh, yeah.

Steve: ...way before the end.

Leo: You'd never write to the end, or – yeah, yeah.

Steve: Exactly. So basically you end up killing this thing way before you need to. But the higher quality Flash has write leveling built in...

Leo: Interesting.

Steve: ...so it's automatically distributing those writes across the entire physical surface of the drive. So it's really worth doing that. These, of course, are not problems for an actual little USB

2.0 hard drive.

Leo: Those little drives you can get, yeah.

Steve: Now, one other thing they recommend – that is, MojoPac recommends – is that the first time, if you're concerned about performance, or if it seems sluggish – I saw no sluggishness at all in my case. I mean, literally, I'm totally happy using this thing for, like, mail, web browsing, newsgroups. For example, with a newsreader in particular, you really want to carry your whole environment around because it's all the messages that you've already read, and all the messages that have occurred, so that conversation threading works correctly. So there, I mean, it's just – it's not the same as going and doing, like, a web-based read of a forum, where it is all being kept over on the server side. But, I mean, I was completely happy with the performance of this thing. However, by default, Microsoft Windows turns off write caching for USB devices. The reason is, if someone yanked it out of the...

Leo: Right.

Steve: ...of the connection, you might well have what's called a "dirty cache" in Windows, where it has been deliberately buffering writes so as not to redundantly write to the device, and also so as not to incur the performance penalty of doing so. So what happens is Windows realizes this is a USB device, and it will turn off write caching. You can go in to, you know, right-click on My Computer, go to Manage, go to find the USB device, select the properties of it. And they explain this in the Mojo ReadMe exactly what the path of clicks is to get there. And then you deliberately turn on delayed writing. That means you need to shut down MojoPac through the UI and not just yank it out. But of course most users know now they really ought to do a smooth shutdown of a USB drive anyway.

Leo: Oh, really?

Steve: Oh, yeah.

Leo: I didn't know that. I thought Windows just kind of, you know, it handled it, so I just pull it out.

Steve: Well, under Windows 2000...

Leo: Well, 2000 you have to do it. But under XP you don't.

Steve: Well, no. And the reason you don't is Windows is still trying to flush it. However, if you've ever done a large file copy, even under XP, the file copy dialogue will finish. And if you've got a light showing access to the device, it'll sit there and flash, sometimes for 30 minutes, because Windows has flushed everything out of its upper UI level, but the kernel is still trying to write to an inherently slow writable device, which is what USB Flash is. So you really need to wait. And what you should do is right-click on the drive appearance in Explorer and then select Eject, and wait for the eject to complete, and then it's safe to remove.

So anyway, my point is that another sort of a power user trick is you could disable, or rather enable, write caching, which is not the default setting for a USB portable device because

Microsoft wants to keep the caches flushed and keep the drive current in case somebody yanks it out without shutting it down. I actually didn't bother with that, and I just saw no performance penalty. I'm really pleased with this.

So again, I want to make sure people understand this is, you know, Version 1.0 – actually it's 1.0.1 at the moment. I believe this thing has a future. I think people are right to be excited about it. And it offers a lot of features. The only caveat being, you know, Windows wasn't designed this way. And so these guys have had to do deep hooks into the kernel in order to pull this off. But I think for most people they have, and it'll only be some people who have problems. So again, use that 30-day eval, or your 200 boots, you know, as quickly as you can within that period, figure out if the things that you think you want to do work without any trouble. And if so, you know, then I think it's a great solution for you.

Leo: Very good. I mean, obviously these guys are filling a perceived need. There's no question about that. And they're amazing hackers. And since it doesn't in any way impinge on your system, why not try it out? Why not give it a shot?

Steve: Yeah, again, it's small and lightweight, doesn't affect your system, and it's, you know, seeing it work is to believe it, Leo. Your attitude, I mean, my attitude changed.

Leo: Well, I've tried it. I mean, I have seen it work.

Steve: Okay.

Leo: Yeah, we tried it out at Call For Help actually, Cali demonstrated it. And it was impressive. It just makes me nervous. MojoPac.com. And as Steve said, you can try it for free.

You know, we've been talking about a free trial version of SpinRite for some time. I think you've really got to try that. You've got to do that.

Steve: I don't know how I would do that. As I said to you before, Leo, you know, we offer it with a complete money-back guarantee.

Leo: I think that's the best way to do it.

Steve: Well, and because the fact is, the first time you use it, you get tremendous benefit from it.

Leo: Right.

Steve: It's not a productivity application like Word or something else, where it's like, okay, do I really want to keep using it after 30 days. In fact, we received a nice note from a Security Now! listener just this week. He said, "I just wanted to give you some more feedback on SpinRite. I've been listening to Security Now! since some of the earliest episodes and have been thinking about getting a copy of SpinRite. Well, I had just the right opportunity this past weekend. A friend's computer started refusing to boot into Windows XP. And I took a good look at it and

found the Maxtor hard drive was going bad, very bad."

Leo: Uh-oh.

Steve: "He had over 8 gigs of digital photos on it that he absolutely did not want to lose. And I was having very little luck trying to copy the files off of it. So I got a copy of SpinRite and ran it" – get this – "for two and a half days straight."

Leo: Oh, my god. See, I think sometimes people give up because they don't realize it could take that long.

Steve: Well, he says he ran it for two and a half days straight, "until we had a power outage."

Leo: Oh, no.

Steve: It's like, okay. He said, "After that, I decided to see what I could recover. And I was able to easily recover all the photos."

Leo: Wow.

Steve: It worked great. So...

Leo: Did you design it to handle a power outage like that? I mean, it fails gracefully like that?

Steve: It fails gracefully. That was something that was tested extensively back in the SpinRite 1.0 days. And, you know, I put in the technology to make it do the right thing. And, you know, two and a half days is extreme. You know, many people talk about it running on 250-gig drives in a few hours, which it's certainly able to do. But, you know, what happens is, I mean, SpinRite is really doing hard work. And...

Leo: It had to do a lot on that drive.

Steve: And when you compare this to taking the drive out and sending it somewhere...

Leo: Right.

Steve: ...two and a half days is much less time than waiting multiple weeks to have some data recovery company fix it for you for way more than $89.

Leo: Very impressive. SpinRite, it's at GRC.com. And if you want to see more testimonials,

it's SpinRite.info. And of course GRC.com is the place to go for 16KB versions of this, for the bandwidth challenged. Also Elaine's great transcriptions, she does those just for you because I know sometimes it's hard to follow. But you can read along as you listen. Again, GRC.com. Visit TWiT.tv. We have an episode guide going back – just as Steve does – going back all the way to the very first episode, so you can see what you've missed. And a lot of people download these shows much later. I think it's the kind of thing people collect, and they want the whole set.

Steve: Oh, Leo, I get postings from people all the time saying that they just discovered us, and they've been listening to all the back episodes. So I'm...

Leo: Yeah, isn't that wild?

Steve: ...really happy that we have that archive.

Leo: Yeah, no, it's a good thing, it's absolutely a good thing to have. If you like Security Now!, you might like Windows Weekly. It's another podcast, this time about Windows, with Paul Thurrott. Very similar style. Paul is a great Windows expert, and we talk about, not specifically security, but just Windows Vista and Microsoft and what they're up to. And of course that's getting very interesting right now. That's also available at TWiT.tv.

Your support is much appreciated. You know, we've had advertising for some time, but as the advertising came on the show, the donations dwindled. That's kind of bad news because, frankly, the donations pay for the infrastructure. The advertising only pays salaries. So your $2, if you like – somebody asked me, well, I like this show, but I don't like that show. Can I just donate to this show? Yeah, just you know, put in your note when you donate the $2, say it's for Steve. That's fine. And I'll make sure that it only pays for the bandwidth that Steve uses. Or something.

Steve: I think I use a lot of bandwidth, Leo.

Leo: I think you do. I think you do. We do thank the great folks at Astaro, who've been a sponsor for so long. Really they came to us and said, we love what you're doing, we want to support Steve, and we'd like to become kind of the flagship sponsor. They make the Astaro Security Gateway, and I think that's a marriage made in heaven for Security Now!. If you're a small or medium business network, you need superior protection from spam, from viruses, from hackers, complete VPN capabilities, intrusion protection, content filtering, an industrial-strength firewall, all in a very easy-to-use, single high-performance appliance, you ought to try out the Astaro Gateway. Contact Astaro.com or call 877-4AS-TARO. You can schedule an absolutely free trial of the Astaro Security Gateway in your business. And for non-business users you can download the software, put it on an old machine. You can even subscribe to all of the things like the antispam and antivirus if you choose to. It really is a great deal. Astaro.com.

Also thanks to Dell for their sponsorship of the show. We have more Dell picks on our special Leo's Picks Page. It's TWiT.tv/dell. Somebody sent me a note saying, "Leo, why do you refer to yourself in the third person like that?" Well, it's just what it's called, the Leo's Picks Page. They are my picks. Dell is at TWiT.tv/dell. And anytime you buy a computer from Dell, if you go through there, we get credit, so we'd appreciate it. Steve, next week we are going to do questions and answers.

Steve: Episode 64, one of my favorite numbers, being that it's a power of two, as well.

Leo: Oooh, yeah. You know, when my kid, my son was, like, six or seven, he said, "Listen, Daddy, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024." And I went, "Wow. Henry, you're going to be good at computers." He said...

Steve: Oh, yeah.

Leo: Yeah. He goes all the way up to – he was at that time going to 4096. I was impressed. I thought, this guy's got a binary brain. He's only shown aptitude so far for YouTube videos, though. So I don't know, maybe it was just...

Steve: You know, just to entertain myself, Leo, I used to practice seeing how far up I can go. I mean, it...

Leo: Really.

Steve: It's pretty scary.

Leo: How high do you, can you – you get up to four million, it gets a little – or four billion, it gets a little tough after that.

Steve: I had it memorized up to, like, 10 or 11 places, I think.

Leo: Wow.

Steve: I mean, decimal digits.

Leo: Wow.

Steve: Just, you know, it's like, you know, some people memorize...