MojoPac: Get your Mojo working

By Russ McRee – ISSA member, Puget Sound (Seattle), WA, USA chapter

Prerequisites

MojoPac device requirements:

Any iPod except the Shuffle, USB 2.0 external hard drive, or USB 2.0 flash drive.

Minimum storage required is 128 MB, 2GB or larger is recommended.

Host PC requirements:

Windows XP (32-bit only)

Vista support currently in beta

256MB Minimum, 512MB recommended

Similar Projects

PortableApps[1]

Introduction

"And now for something completely different." For your consideration, MojoPac Freedom.[2] MojoPac is an offering from RingCube Technologies that transforms your iPod or USB drive into a portable and private PC. One simply installs MojoPac on any USB 2.0 compliant storage device, uploads applications and files, modifies user settings and environment preferences, and you're off to the races, "just like mojo hand."

Never did you imagine your author sneaking in both a Monty Python reference and Grateful Dead lyrics in the same paragraph, let alone the same column, but alas, I could not pass on the opportunity. Rare is the chance to hone one's security mojo to such a heightened state, so let us endeavor to do so.

Each time you plug your MojoPac-enabled device into a Windows XP PC, MojoPac automatically launches your environment on the host PC. This is interesting enough with your communications, music, games, applications, and files all available from your USB device, while borrowing resources from the local host, but consider this all from a security perspective.[3]

"MojoPac provides several layers of security and isolation to protect the Mojo user:

- When you connect to a Host PC, MojoPac provides a layer of isolation against viruses from the Host PC, so your MojoPac device is protected.
- MojoPac creates a private environment, so none of your application data and settings, including your browsing and multimedia player history is stored on the Host PC. Privacy buffs rejoice. What happens on MojoPac stays on MojoPac.
- MojoPac is password protected; if you lose your device, no one else can access your applications.
- In addition, data encryption is supported within MojoPac either by add-on encryption software or by using a USB storage device that directly encrypts the data stored on the device. Some USB storage devices even have built-in finger print readers for added security. We recommend using data encryption with every portable storage device."[4]

As an incident handler, investigator, analyst, or administrator, you have read me saying more than once that using "trusted" tools and applications is essential to a successful response or investigation. Imagine walking into a "hostile" client environment with your MojoPac-enabled device while leveraging a host PC's resources and conducting remote analysis of other systems or even the host PC (in contradiction to the vendor's claims). MojoPac virtualizes the registry, files system, and security services but avoids virtualization in the true sense in that it is not virtualizing hardware.

RingCube is looking to offer Vista support later this year. As is the norm for most vendors, the free offering leads way to a commercial version, in this case, MojoPac Enterprise. Should you choose to purchase, you will be treated to the following:

- Web-based user portal (i.e., web-based delivery of MojoStation)
- Enhanced isolation capability
- Endpoint security checking
- Ability to prohibit application installation within MojoPac
- User revocation (e.g., disabling lost/stolen MojoPacs)
- Cisco VPN & Juniper VPN support

1 http://portableapps.com.

2 http://www.mojopac.com/portal/content/hellomojo.jsp.

3 http://www.mojopac.com/portal/content/what.

4 http://www.mojopac.com/portal/content/how/security.jsp.

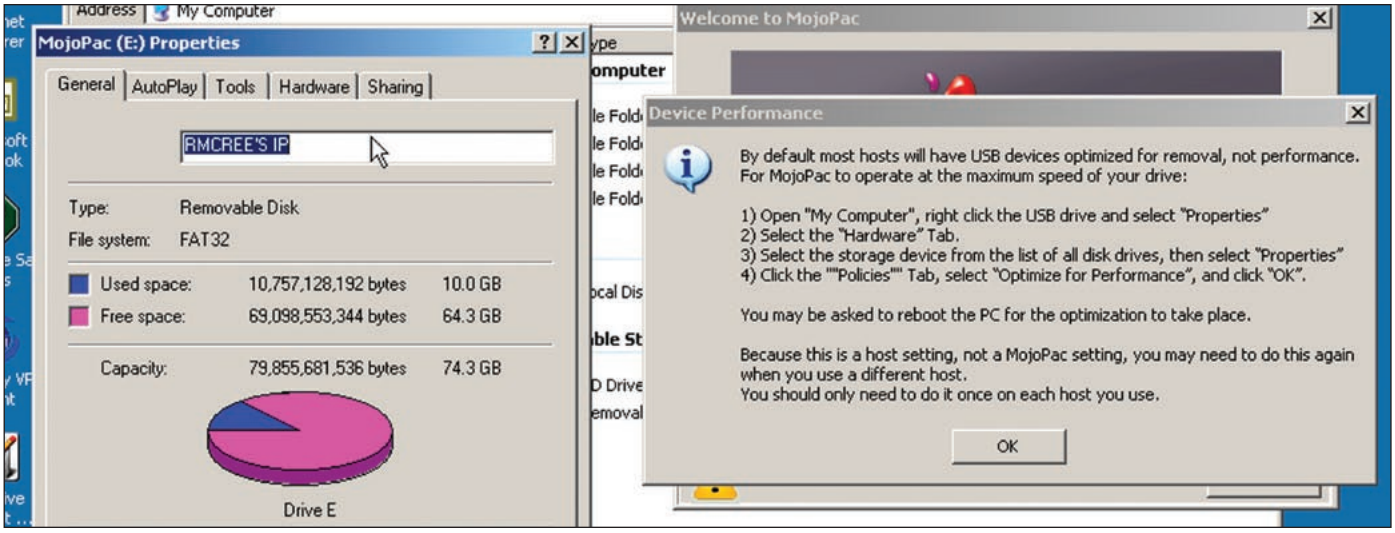

Figure 1 – Optimize for MojoPac

- Protect Storage support (i.e., client certificates)
- Data Sync between host & guest (e.g., sync browser bookmarks, My Documents, etc.)
- Centralized management (admin server)
- Active Directory integration for authentication and authorization

MojoPac installation

I installed MojoPac on the data partition I keep on my iPod, and it was a very straightforward process. I accepted defaults, assigned my super-Mojo password and was immediately under way.

I certainly recommend optimizing your hardware before you install security applications of your choosing. Mojo's kind enough to assist in the process. See Figure 1.

MojoPac use

In your MojoView, your "C" drive represents your MojoPac device, NOT the Host PC's hard drive. So applications install in the right place on your MojoPac device automatically.

That said, while RingCube suggests that you cannot access the host PC files and folder from your MojoView, when I mounted \\192.168.1.101\C$, I gained immediate access to the *host PC* C: drive. This could be useful if your host is compromised in some fashion and you need to play "find the malware."

I did not test MojoPac under these circumstances, and I am therefore uncomfortable green lighting your doing so without the following caveat: RingCube says you should not be able to do this, thus their claims of "isolation" in the Freedom version are a bit overstated. I am reasonable comfortable, however, saying, you will not have much luck jumping from the host PC to your directly to you MojoPac file system.

From the MojoPac forum I learned that "MojoPac inherits the TCP/IP settings from the host PC and all the security settings and policies on the host PC will be applicable on MojoPac also." This, in part, explains the ability to mount the local host drives from the admin share, but it also allows you to capture traffic from the host PC. Again, it is not as isolated as RingCube likely intended, but it is useful for the incident responder.

Random thought: if MojoPac and the host PC share the TCP/IP stack, how will the Windows Firewall interact between the host PC and MojoPac Freedom? I will add it to my list of things to break and report later.

All claims of isolation aside, if you are reasonably certain that a host PC in your target environment is clean, plug in your MojoPac device and get busy on remote hosts, content in the knowledge that your MojoPac installed, trusted security tools are running from the MojoPac installation while taking advantage of host PC resources.

My MojoPac includes the following – by all means optimize your MojoPac to your liking. Remember, when in your MojoView, the apps you install are installed to your MojoPac. It is really like a new instance of XP altogether, registry included. There are some limitations to what will run in your MojoPac, but I installed and successfully ran these:

- ClamWin
- Helix IR tools for Windows, including PS Tools
- Nmap
- Wireshark – Again, because you are sharing the host PC's TCP/IP stack, if it is owned and calling home you can capture outbound traffic from the host.

Once I had all my applications installed and tuned to my liking, I was able to scan and analyze remote target hosts on my lab network quite successfully, as if I were engaging directly from the host PC. The MojoView tool bar resides at the top of your screen and easily allows you to bounce between MojoPac and your host PC. See Figure 2.

If I were spend a lot of time with this tool, I would likely add some additional tools: Nessus, Nikto, RAPIER, the Metasploit framework, and others, just to have everything I might ever

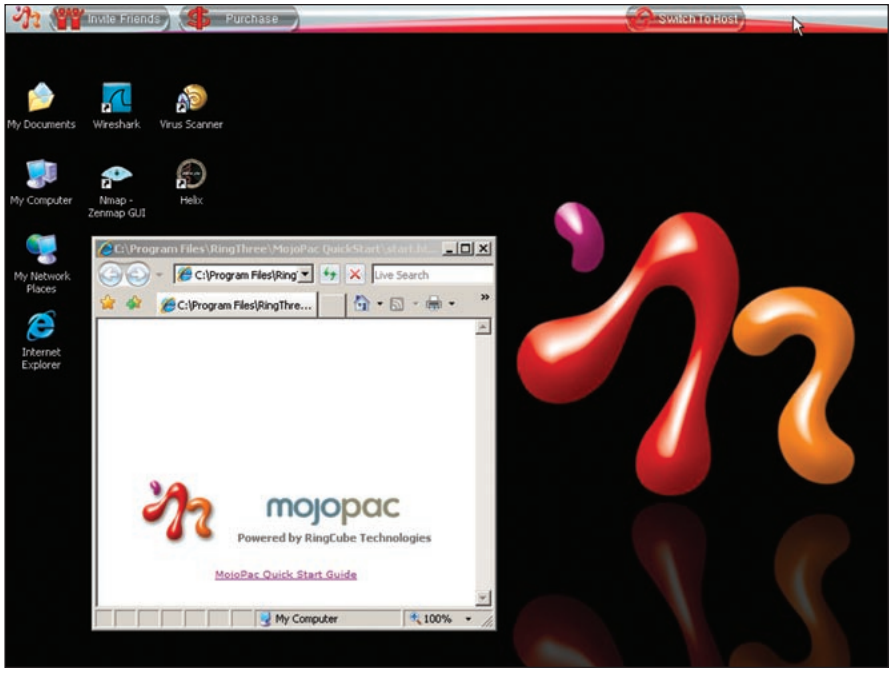

Figure 2 – MojoPac ready to do the hoodoo

need in a highly portable platform. Everything I loaded worker quite well; but of all the tools I loaded, I found the Helix Windows IR tools most useful.

Benefits and drawbacks

This is a great little app, and a novel idea, but a bit heavy handed in its claims of isolation. I agree that the apps running in MojoPac run from the USB device while taking advantage of the host resources, but the fact that TCP/IP use is so interwoven, putting a hefty hurt on your host PC from your MojoPac is definitely possible. What seemingly will not happen is trouble coming the other way, from host PC to MojoPac; it definitely seems to remain shielded. Regardless, I like the idea of portability and a "trusted" environment from which to run my tools. Even fully optimized my MojoPac runs a bit slowly but still significantly outperforms rebooting a host PC to utilize a LiveCD like Helix or BackTrack. For that matter, it runs faster, with less CPU and memory, than running a full guest Windows VM on top of the host OS on VMWare, Virtual PC, or Parallels

In conclusion

Keep MojoPac on standby. It may not become a premier tool, for support and development seem a bit spotty, but it definitely has its place. When you have hardware or resource limitations, being able to walk into a hosed corporate desktop environment and conduct a successful investigation or response via your USB device, and being able to run you apps in isolation, is rather unique. Enjoy experimenting and let me know how it works for you.

Cheers, until next month…

Anytime you would like to email me with questions, comments, or feedback regarding toolsmith and your experience with the tools we discuss, please do so to holisticinfosec@gmail.com.

Acknowledgement

Doug "Tom" Dooley (sorry, another Grateful Dead reference I couldn't resist) for taking the time to enlighten me regarding MojoPac Freedom and RingCube offerings.

About the Author

Russ McRee, GCIH, GCFA, CISSP, is a security analyst working in the Seattle area. As an advocate of a holistic approach to information security, Russ' website is holisticinfosec.org. Contact him at russ@holisticinfosec.org.