Technical White Paper: Running Applications Under CrossOver: An Analysis of Security Risks

codeweavers

Wine, Viruses, and Methods of Achieving Security

Running Windows software via CrossOver is, on average, much safer than running them under Windows

Overview: Wine is a Windows compatibility technology that allows a wide variety of Windows software to run as-if-natively on Unix-based operating systems like Linux and Mac OS X. From a theoretical standpoint, Wine should also enable malware and viruses to run, thereby (unfortunately) exposing Wine users to these same hazards. However, CrossOver (based on Wine) also incorporates security features that bring this risk down to almost zero. This White Paper examines the reasons behind the enhanced safety that CrossOver provides.

With the increasing popularity of running Windows software on Linux and Mac OS X via compatibility solutions such as Wine, VMWare, and Parallels, users have been able to enjoy a degree of computing freedom heretofore unseen. Yet with that freedom has come peril. As many VMWare and Parallels users have discovered, running applications like Outlook and IE under those PC emulation solutions also opens up their machine to the same viruses and malware they faced under Windows. Indeed, one of the first things any VMWare or Parallels customer should do upon is install a commercial anti-virus package. Failure to do so can result in a host of dire consequences for their Windows partition, just as it would if they were running a Windows PC.

Not surprisingly, a question we sometimes hear is whether or not Wine exposes users to the same level of risk. The short answer is: *in theory*, perhaps; in practice, no. That is, a virus could theoretically infect a Unix-based system (either Mac OS X or Linux) running a Windows program, but it would require an extremely unlikely scenario for that to happen. To our knowledge, it has *never* happened. As a result, we maintain that it is far safer running Windows software under CrossOver than it is running them under Windows. Why is this? The answer lies in both the superior security of Unix-based operating systems, which makes it extremely difficult for viruses to run, as well as active steps we have taken to make CrossOver more secure.

Viruses vs. Unix-based Operating Systems

A Wine user's first line of defense against viruses is that they simply don't run under Wine. Why is this? After all, in theory, programs that are vulnerable to virii—such as Outlook and Internet Explorer—will retain those same vulnerabilities when running via CrossOver. And if a Windows virus exploits a weakness in Internet Explorer which allows it to upload code into memory and cause that code to start execution, then that same weakness will theoretically exist under Wine as well. Yet, again, in practice we have never run into a single instance of this happening. On the face of it, this seems incredible. Wine, after all is designed to be a general-purpose Windows compatability solution. And while it doesn't run *all* Windows software yet, it *does* run a respectable percentage of them. It would seem reasonable to assume that at least *some* Windows viruses would run as well. Why don't they? The answer has to do with the specific nature of malware applications, and how they interact with their target operating systems.

Windows viruses take advantage of specific chinks in the armor of Windows. Those same vulnerabilities largely do not exist under Unix-based operating systems.

When you are running an application under CrossOver, CrossOver serves as the intermediary between the application and the operating system. Wine is constantly taking in requests from the application for services, via the Win32 API (which is Wine) and then translating those Windows requests into something intelligible by the target OS (Linux or Mac OS X). Under normal circumstances, Wine processes these requests seamlessly, and the target OS satisfies the needs of the program.

By their very nature, though, Windows viruses are built to take advantage of specific security holes in Windows. They rely upon a very exact operating system configuration, and use certain Windows-specific commands to do their dirty work. What happens when a piece of Windows malware tries doing that under CrossOver, though, is two-fold. First off, the vast majority of the time the executable just doesn't run. But even more important, the chinks in the armor of Windows that the malware is trying to address typically make no sense to a Unix-based OS. In most cases, the particular weakness the virus is going after probably doesn't even exist in Unix.

Could a virus be written that would work under Wine? Again, theoretically yes. But writing a virus to attack, say, a Mac via CrossOver would require that 1) it went after specific security flaws in the Mac OS, but also 2) ran as a Windows executable, that 3) also ran flawlessly under CrossOver. That's a very tough bill to fill. This is not to say that it wouldn't be theoretically possible to do, but in practice it's very, very difficult.

Even if such a virus were crafted, it would still be constrained by the Unix system as to the damage it could do. Since CrossOver is

meant to be run by a regular user, the user is protected by Unix's security system. A Windows virus would generally only know of the Windows file systems (which under CrossOver is confined to a virtual C: drive located in two separate directories under the user's home directory.) If the C: drive were somehow to get infected, that infection would find it very difficult to get into either the user's other directories, or into the root file space.

Even better, your personal data (your documents, videos, etc.) need not reside on Wine's virtual C: drive at all. After all, one of the benefits that Wine provides is being able to use the native file system of the host computer, meaning that your personal data most likely won't be stored on the virtual C: drive in any case—it will be located whereever you normally put your document files under, say, OS X. Disinfecting a Wine C: drive is extremely easy, too. Simply deleting the pair of CrossOver directories housing the C: drive destroys the infection completely.

A reminder to our customers: you're only vulnerable if you run vulnerable applications. We strongly advocate the usage of Firefox except for those sites that absolutely require Internet Explorer.

CrossOver's Interaction with other Security Software

The second major line of defense for any CrossOver customer is that CodeWeavers has taken active steps to enhance Wine's security by providing CrossOver with number of mechanisms to either interact with other security applications, or to detect and disallow the running of any questionable code.

First of all, CrossOver allows a system administrator to install all the Outlook service packs and updates that s/he would normally install as part of a rigorous approach to Windows security. In other words, CrossOver gives a user access to all the tools that Microsoft provides to ensure the security of its own products.

A second facility that CrossOver provides is the ability to interact with local and server-based anti-virus software. Just as a Windows user can have their email checked by commercial anti-virus software, so too CrossOver has the necessary "hooks" to allow Outlook to be monitored by, say, a Linux-based anti-virus package. Thus, CrossOver replicates all the facilities that a Windows user has to protect themselves. However, because of the power of Unix, we can actually take this several steps further.

By default, CrossOver will have any item placed in the system's temporary directories scanned (which is typically where email attachments are placed before they are opened). However, a third facility CrossOver has is the optional ability to require scanning of *any* item that is opened. Thus, CrossOver provides a facility that Windows itself does not provide—the ability to *force* a scan of any/all items at the user's discretion.

A fourth and final facility that CrossOver customers can take advantage of is using CrossOver's Managed Multi-user Mode and running applications in a 'chroot' jail. Under this mode of operation, all Windows applications are installed into a read-only area on the drive. This read-only area is temporary, and is erased prior to every invocation of the application in question. This mode of operation absolutely guarantees that no virus could harm anything outside of the 'jail.' We don't actually recommend this approach because we don't feel its necessary and it makes working with files awkward. However, this is an absolutely safe method for those customers that are genuinely concerned about the possibility of viruses.

CrossOver allows the creation of tailored security environments that, at their most rigorous, are practically unassailable.

Finally, we remind our customers that you're only vulnerable if you run vulnerable applications. Internet Explorer is a magnet for malware. As a result, we advocate that users switch to Firefox whenever possible, and only use IE for sites where Firefox simply does not work (which is becoming increasingly less common in any case.)

Outlook, of course, is the other prevalent source of incoming viruses. However under CrossOver, Outlook is prevented from running files with typical virus file formats. This is an outstanding example of customizing an open-source technology in the best interests of the user. Normal Windows won't prevent users from doing this sort of thing, but since actual users control the development of Wine, it has been crafted in such a way as to prevent virus and malware attacks.

To summarize: Running Internet Explorer and/or Outlook under CrossOver is not only safe, it is *more* safe than running those same applications under Windows. Using CrossOver presents viruses and malware with an OS "target" that is very difficult to attack in the first place. So difficult, in fact, that we know of no case where a virus has actually run under Wine. But CrossOver also provides additional facilities that raise the bar still further, and in a user-configurable fashion. CrossOver allows its users to establish whatever level of security they desire. Indeed, for those customers with very high security needs, the special "hooks" inside CrossOver allow for the creation of customized, secure work environments that are practically unassailable—something that no Windows solution can provide.