

This Free E-Book is brought to you by Natural-Aging.com.



The Risks of Desktop Security Software – Part 1

By Tim Klemmer

The Risks of Desktop Security Software – Part 1 by Tim Klemmer

This is the second in a series of articles highlighting reasons why we need a new model for anti-virus and security solutions.

Reason #2: the Desktop Security Software Risks

The risks of placing software on the desktop are such that I will be breaking this article into two parts.

Fundamentally we think of having software on our desktops as a good thing. I love downloading or installing new packages and seeing what new creative things people do to the user interface or what they do to make certain aspects of my life easier or more fun.

But there are problems inherent with software that resides on the desktop, especially security software. All developers will know what I mean. First and foremost, desktop software can be reverse engineered. What's that mean? Have you ever inadvertently double-clicked on a file and had garbage show up or seen something that looks similar to this?

The old hex dump. Programmers will know it well. We actually spend a good deal of time trying to read this stuff. Basically, if there are programs that can (and do) turn instructions like the following

```
If UserBirthDate IsReallyOld = "Yes  
Else  
IsReallyOld = "No"  
End If
```

into something like the picture above, then the reverse is true: people have developed software that can take that gobbledy-gook in the picture above and turn it somewhat into the if-statement I wrote out. The reversing software won't know that I had an item called UserBirthDate, but it will know I was testing for a value of January 1, 1960 and it will be able to say that based on that value I set another item to Yes or No.

The Risks of Desktop Security Software – Part 1

So now we install our fool-proof anti-virus software on our desktop (or our firewall for that matter). Well, so too can a virus author. And that virus author or hacker will also have gotten a copy of the latest reverse-engineering software from his local hacking site. He now goes upon his task of reverse-engineering the software and then trying to decipher the results. It's not easy but it can be done. Unfortunately, vendors know this and understand this as an acceptable risk.

The problem here is that your security software is at risk. If your vendor codes an error, the virus author can and will detect it. For example, if your vendor should exclude a file from scanning, it's possible the virus author will figure out which file (or type of file) that is and bury his code there. If the

vendor excludes files from scanning or heuristics, it's possible that virus author will figure out a way to corrupt that file.

That being said, there are other risks. As we have said, once software is on the desktop it affords virus authors an opportunity to reverse-engineer security software. The knowledge that reverse-engineering provides is invaluable to a virus author when building his next software attack. Third, virus authors can learn where the anti-virus vendors put their software and put the links to their software (directory folders, registry entries, etc.). This too is invaluable information. In fact, in some ways it teaches people intent on writing malicious software clues as to how to infiltrate the computers' operating system, where registry entries need to be made to force software to be loaded every time a computer is started, etc.

This information is generally available all over the web and in manuals for operating systems, especially manuals on such subjects as the Windows Registry. But having the software teach you where things belong to be effective is powerful knowledge.

Lastly, and perhaps most significantly, is the issue of forbearance. The anti-virus vendors usually know more about the potential exploits inherent in programs than virus authors but they are bound by the fact that should they try to prevent them before the exploits occur, they could be branded as irresponsible for teaching virus authors about these very exploits.

For example, when Microsoft first released the macro capabilities of Word, anti-virus vendors immediately realized the potential for danger in macros, but they were handcuffed. If they released software that disabled macros before the first macro virus was ever released, they would signal to virus authors the inherent destructive powers of macros. They chose instead to wait, handcuffed by the limitations of desktop software.

Until the Internet there really has been no better medium for delivering virus solutions than desktop software. It was relatively inexpensive to deploy (either market the software and sell it in stores or provide free downloads on bulletin boards and web sites). It is, however, expensive to keep updated in terms of time and effort, even with automated update systems.

The Internet caused several things to happen: by becoming a powerful medium for sharing files, whole families of viruses disappeared practically overnight (boot sector viruses, for example); by becoming the option of choice for sharing files, it was easier to infect a single file and have thousands download it.

The Risks of Desktop Security Software – Part 1

A better solution is to place the security software in an offsite appliance of its own making. All Internet, intranet, networking connections flow through the appliance.

Selling off the shelf hardware appliances with built-in security software is better than a desktop software solution but it still suffers -to a lesser extent- from the pratfalls that desktop software falls prey to.

Even better is to create a service that a 3rd party vendor manages in a secure environment. In such an instance both the software and the hardware are away from the prying eyes of the malicious software authors. This further reduces the opportunity for malicious authors to discover the tricks and techniques employed by the security vendors to protect you.

Tim Klemmer CEO, OnceRed LLC <http://www.checkinmyemail.com> Tim Klemmer has spent the better part of 12 years designing and perfecting the first patented behavior-based solution to malicious software.

Desktop Security Software Risks – Part 2

By Tim Klemmer

Desktop Security Software Risks – Part 2 by Tim Klemmer

This is the third in a series of articles highlighting reasons why we need a new model for anti-virus and security solutions.

Reason #2: the Desktop Security Software Risks

The risks of placing software on the desktop are such that I will be breaking this article into two parts.

There are many advantages to putting security and anti-virus software on the desktop. They range from efficiency to money. Under previous ways of thinking if I can capture security and virus problems at the desktop I can prevent them from going any farther. That works well in a non-connected environment. In the connected environment it makes more sense to centralize the software and monitor connections in and out. Basically "firewall" all the appliances from each other.

In a previous article we discussed the security risks inherent with desktop software designed to be the protection layer between you and all those bad people out there on the Internet. Here now we will discuss some more mundane issues regarding the risks of putting security software on the desktop:

Drag

Drag steals clock-cycles from your processes so that it can run in a higher priority mode. Anti-virus software especially places a drag on your computer. Depending on your settings (and the default settings are usually very aggressive), every time you run a program or open a file, real-time file scanning takes place and your files are scanned for viruses. This slows down your processing. Accessing larger files takes longer. You can see a discernible lag time between when you start a

program/open a file and when you can actually access it.

Compatibility

After the obvious issue of "drag" is compatibility. Often security and anti-virus rules get in the way of your doing business on your computer. While you may get away with using older versions of such packages as Word, Sims, Photoshop, etc. on your computer with the new XP operating system, it's unlikely your security software will be completely compatible. Why? Many packages rely on very low-level functionality to be able to do the tasks they set out to do. Anti-virus packages have to be able to operate at a level closer to the hardware than most packages. They need to do this to prevent virus software from taking precedence from them. While many packages offer backward-compatibility the opposite is not true: forward-compatibility. There are several reasons for this: a package written for Windows 98 will not anticipate all the changes to the operating system that are implemented for Windows XP. While your Win98 anti-virus program may work under XP, it won't work at its peak performance. It can't. It's just another reason for centralizing your security. By siphoning all your traffic through a security screen at your ISP, for instance, you offload the need for updates and staying up-to-date on your security software. This then becomes the job of the service provider.

Updates

Having the software on your desktop means you are responsible for maintaining that software. In the case of office productivity software or image editing software, if new versions come out with features you're not interested in, you don't update. With new viruses appearing on the landscape every day, you

can't afford not to continually update your software. If you don't update for a month or two, you run severe risks of infection. You also will incur potential long update cycles as your software has to be upgraded to handle all the new threats.

This makes the desktop these days a somewhat ineffective solution. Nearly two-thirds of all the PCs that have anti-virus protection installed do not update their definitions regularly. These PCs might as well uninstall the software for all the good it's doing them.

Lost Time

As mentioned in the above discussion, you can lose considerable time if you don't update regularly. Long intervals between updates can translate into long update cycles. If you have a slow connection to a vendor, your down time is much longer as you have to wait for the files to be downloaded and then you have to wait for your software to update itself.

Solution

The better solution is to move to a centralized solution in which all the software, all the updates are the responsibility of the service provider. You pay for the service of having your email cleaned before you receive it. When email arrives at your service provider's mailbox, it is checked for malicious tendencies and stripped if bad. You notice no long waiting, no downtime, no drag, no incompatibilities.

Tim Klemmer CEO, OnceRed LLC <http://www.checkinmyemail.com> Tim Klemmer has spent the better part of 12 years designing and perfecting the first patented behavior-based solution to malicious software.



This Free E-Book has been brought to you by Natural-Aging.com.

[100% Effective Natural Hormone Treatment](#)
Menopause, Andropause And Other Hormone Imbalances
Impair Healthy Healing In People Over The Age Of 30!