

News for nerds, stuff that matters

- [Login](#)
- [Create Account](#)
- [Subscribe](#)

- [Why Login?](#)
- [Why Subscribe?](#)

Log in

Nickname

Password

Public Terminal

Log in

[[Create a new account](#)]

Opinion Center: [Intel](#)

Symantec Will Not Detect Magic Lantern

Posted by [timothy](#) on Wed Nov 28, '01 01:37 PM
from the et-tu-eric dept.

An anonymous reader contributes: "In [this article](#) on Declan McCullagh's Politech, [Symantec](#) chief researcher Eric Chien stated that provided a hypothetical keystroke logging tool was used only by the FBI, Symantec would avoid updating its antivirus tools to detect such a Trojan, echoing a similar stance Network Associates [allegedly took](#) with its McAfee anti-virus software [earlier this week](#). 'If it was under the control of the FBI, with appropriate technical safeguards in place to prevent possible misuse, and nobody else used it -- we wouldn't detect it,' said Chien. 'However we would detect modified versions that might be used by hackers.'"



NEED TO START A WEBSITE?
....OR JUST NEED A BETTER HOST?

- 5GB DISK SPACE
- 50GB BANDWIDTH
- 50 SUB DOMAINS

DEVELOPER TOOLS All Inclusive **\$6.95/mo**

OLM.net 10 YEARS HOSTING WITH AWARD WINNING SERVICE

(1) | 2

- [No need to use Norton AV...](#) by the_rev_matt (Score:3) Wednesday November 28, @01:39PM
 - **Re:No need to use Norton AV...**

(Score:4, Insightful)

by [babbage \(61057\)](#) <cdevers@@@cis...usouthal...edu> on Wednesday November 28, @02:07PM (#2625476)

(<http://devers.homeip.net:8080/blog/> | Last Journal: [Tuesday April 12, @09:34AM](#))

...until of course the first big cross platform or Linux only virus comes along and trashes your computer[s], which we all know is just a matter of time.

Your OS is certainly more esoteric, but it has holes like all the rest of them do. Your immunity thus far isn't an indication that there are no holes -- there are *always* holes -- but that the *nix environment hasn't yet been able to cultivate & propagate any really serious viruses yet.

One of two things is likely to happen: Linux's popularity will crest & wane, and people will stop using it (unlikely, I hope :), or it will continue to get more popular, and as it does so it will provide an ever more appealing target for virus writers, licking their chops at all the complacency out there....

[[Parent](#)]

- [Re:No need to use Norton AV...](#) by quartz (Score:3) Wednesday November 28, @02:15PM
 - [Re:No need to use Norton AV...](#) by Anonymous Coward (Score:1) Wednesday November 28, @02:27PM
 - [aga..](#) by Axe (Score:1) Wednesday November 28, @04:09PM
 - **2 replies beneath your current threshold.**
- **Re:No need to use Norton AV...**

(Score:5, Insightful)

by [babbage \(61057\)](#) <cdevers@@@cis...usouthal...edu> on Wednesday November 28, @02:43PM ([#2625731](#))

(<http://devers.homeip.net:8080/blog/> | Last Journal: [Tuesday April 12, @09:34AM](#))

Yeah. Sure. Just make sure you leave enough of whatever it is you're smoking in that pipe so that we can all get as addled as you are on this one.

Mac OSX is becoming an interesting case study in Unix For The Masses. Default Linux is, as the Register recently noted, [from memory, can't find a link] "a paragon of Stalinistic control freakery", and that *has* made it more secure out of the box than the average WinME box, but more importantly it has also scared off millions, and rightly so. Apple's engineers knew well that if they wanted to bring this architecture to the masses -- the way the Gnome & KDE folks do -- then they'd have to encapsulate & hide as much of that control freakery as possible.

And for the most part they've done a good job, but there have been some serious glitches, like programs that would launch themselves as root, or a broken iTunes installer that wiped out whole disk partitions because of one mistyped "rm" command in an installer script. Pay attention, you seething Linux hordes, because if you want to hit the big time then this is your future. You too will face these problems as the system matures & seeks out a wider audience.

The *only* "secure" system is either (pick your punch line) the one that hasn't been built yet, or the one you bought a decade ago and still haven't plugged in yet. All of the others -- *all* of them -- have problems of one kind or another, and all of them always well. Welcome to real life, kids.

[[Parent](#)]

- [Re:No need to use Norton AV...](#) by quartz (Score:3) Wednesday November 28, @03:43PM
 - [Re:No need to use Norton AV...](#) by babbage (Score:2) Wednesday November 28, @04:02PM
 - **1 reply beneath your current threshold.**
- [Re:No need to use Norton AV...](#) by dasunt (Score:2) Wednesday November 28, @02:44PM
- **Re:No need to use Norton AV...**

(Score:5, Informative)

by [Zeinfeld \(263942\)](#) on Wednesday November 28, @03:52PM ([#2626218](#))

(<http://dotfuturemanifesto.blogspot.com/>)

It is NOT only "a matter of time". If Linux programmers will ever get the idea to make Linux login as root by default, to write email clients that allow scripts to be executed without user's permission, to ship their OS without a firewall mechanism in place and to make the whole system a sitting duck to any running script via a conveniently accessible registry file, THEN you will start seeing viruses for Linux. But by then us security conscious people will have long since moved on to another more decent OS.

Don't be so sure. We have had UNIX worms and even VMS worms. Unlike the designers of UNIX, VMS started with a security architecture and actually recieved B2 certification rather than describing itself as 'B2 equivalent'.

At the other end of the scale the security architecture of MAC O/S has until a few months ago been stuck at the MSDOS level, lacking even protected memory, yet MAC viruses are none too common these days.

The significant factor is the proportion of the network population that uses a particular O/S. As with a biological infection there are definite inflection points that determine whether a virus spreads fast enough to cause an epidemic or a pandemic.

When the Wang Worm hit it could propagate because close to 100% of the computers on HEPNET were VMS systems. Equally the Moriss worm took out the Internet when the vast majority of nodes were UNIX boxes running sendmail.

The proportion of UNIX machines on the Internet today is probably close to critical mass for allowing a viral epidemic. The saving factor is not the design of the O/S, it is the variation between the O/S implementations. Anyone who thinks that sendmail is a lesser security risk than Outlook should read a few CERT advisories.

The separation of administrative privs is not actually significant when it comes to the propagation of email viruses. If that was the case Windows XP would solve the virus problem completely (it won't). The problem is that the boundary between code and data has been blurred. For some reason the people who felt they had to foist Java and Javascript winky-blinky features on the world had no clue when it came to security. (Don't get me started about the Java sandbox model, the code does not match the marketing hype, the implementation does not correspond to what I would regard as a sandbox design)

The other reason that UNIX boxes tend to be more secure is that the use of winky-blinky features is nowhere near as widespread. The proportion of terminally clueless users in the Windows world is (acording to my studies) approximately 92.931%, in the Linux world that figure is only 23.428%. So not only is the userbase smaller, the propability that a user sent the virus will execute the program and cause it to replicate is much smaller.

Again, look at biological models of propagation. x^n is a very big number if $x > 1$, it is a very small number if $x < 1$. Therefore the day that AOL ships AOL for Linux will be the day that Linux will start to get virus problems. It will have the active code to support winky-blinky features and thus be vulnerable to attack, it will introduce the terminally clueless into the Linux user base.

[Parent]

- [Re:No need to use Norton AV...](#) by pyros (Score:2) Wednesday November 28, @02:51PM
 - [Re:No need to use Norton AV...](#) by Anonymous Coward (Score:1) Wednesday November 28, @04:43PM
- [Re:No need to use Norton AV...](#) by Asic Eng (Score:2) Wednesday November 28, @03:07PM
- [Not likely at all.](#) by Pinball Wizard (Score:3) Wednesday November 28, @03:44PM
 - [Re:Not likely at all.](#) by jazman_777 (Score:1) Wednesday November 28, @07:51PM
- [Re:No need to use Norton AV...](#) by iabervon (Score:2) Wednesday November 28, @05:31PM
 - [Re:No need to use Norton AV...](#) by flewp (Score:1) Wednesday November 28, @06:52PM
 - [Re:No need to use Norton AV...](#) by iabervon (Score:2) Friday November 30, @12:47AM
- [Re:No need to use Norton AV...](#) by Ogerman (Score:2) Wednesday November 28, @07:25PM
- [Re:No need to use Norton AV...](#) by goodtim (Score:1) Wednesday November 28, @08:42PM
- [Re:No need to use Norton AV...](#) by redcliffe (Score:1) Wednesday November 28, @09:36PM
- [Re:No need to use Norton AV...](#) by n4t3 (Score:1) Wednesday November 28, @11:23PM
- [Re:No need to use Norton AV...](#) by lobsterGun (Score:1) Wednesday November 28, @02:41PM
- [I run Linux and it IS an issue!](#) by SomethingOrOther (Score:1) Wednesday November 28, @03:42PM
 - [Re:I run Linux and it IS an issue!](#) by darnellmc (Score:1) Wednesday November 28, @06:41PM

- [2 replies](#) beneath your current threshold.
- **Uh, the answer is simple...**

(Score:4, Insightful)

by [Nijika \(525558\)](#) on Wednesday November 28, @01:40PM ([#2625280](#))

(<http://google.com/> | Last Journal: [Saturday May 13, @11:28PM](#))

Someone will just write something that in theory WILL detect Magic Lantern. We just have to wait for it. Who in the geek community would really sit back and WAIT for a virus software company to come up with a solution like that.

Anyway, I don't use Windows, so this is not my problem. Ask yourself; is it really yours? :-)

- [Re:Uh, the answer is simple...](#) by Anonymous Coward (Score:1) Wednesday November 28, @01:45PM
 - **1 reply** beneath your current threshold.
- **Re:Uh, the answer is simple...**

(Score:5, Insightful)

by [czardonic \(526710\)](#) on Wednesday November 28, @01:56PM ([#2625391](#))

(<http://slashdot.org/>)

yway, I don't use Windows, so this is not my problem. Ask yourself; is it really yours?

Here's why it IS your problem. If you think the FBI is going to limit their spying to Windows, you are pretty naive. Count on one of the following:

They will find a way to make it work in every consumer OS.

They will find some other way to acheive the same thing with other OSs.

They will outlaw the use of an OS that can be used to evade law enforcement.

[[Parent](#)]

- [Re:Uh, the answer is simple...](#) by sqlrob (Score:2) Wednesday November 28, @01:59PM
- **Re:Uh, the answer is simple...**

(Score:5, Insightful)

by [bfree \(113420\)](#) on Wednesday November 28, @02:13PM ([#2625514](#))

Sometimes the UScentricities of /. just make me ROFL!

All that is happening here is that

- All non-US parties will purchase non-US anti-virus software losing the US anti-virus software produces \$xxxxxxxxx/annum and meaning the US software will have a smaller user base and be more likely to be less secure
- Every US citizen will have to decide whether to break the law (cause I believe they will outlaw the use of anything which cannot be cracked by the FBI, including all the non-US anti-virus products) or to leave themselves vulnerable
- The US will spend a massive amount of resources on trying to control this whole issue. The filtering of the Net would be an immediate requirement to try and find people who are using illegal software, or downloading it
- MY OS will NEVER be vulnerable!! I will always, from some day about 3 years ago, use an OS which is Free where the code can be reviewed, modified and distributed. I can attach hooks into my TCP-IP stacks, network device drivers or any other level I wish to watch for the FBI (or anyone else) trying to track me (or gather any info) and block them at source, but I won't need to cause a 17 year old scandinavian will release a tool to do it for me which will be plastered over the non-US internet
- The US is well on its way to writing itself out of the rest of the world, and whatever they believe they can't survive alone!

Sometimes I honestly feel pity for Americans!

[Parent]

- [Re:Uh, the answer is simple...](#) by czardonic (Score:1) Wednesday November 28, @02:26PM
 - [Re:Uh, the answer is simple...](#) by bfree (Score:2) Thursday November 29, @10:28AM
 - **1 reply** beneath your current threshold.
 - **1 reply** beneath your current threshold.
- [Re:Uh, the answer is simple...](#) by DarkZero (Score:2) Wednesday November 28, @02:52PM
 - [Re:Uh, the answer is simple...](#) by innocent_white_lamb (Score:1) Wednesday November 28, @06:53PM
 - [Re:Uh, the answer is simple...](#) by cyril3 (Score:1) Wednesday November 28, @07:59PM
 - [Re:Uh, the answer is simple...](#) by bfree (Score:2) Thursday November 29, @10:23AM
 - [Re:Uh, the answer is simple...](#) by Logi (Score:1) Monday December 03, @08:19AM
- [Re:Uh, the answer is simple...](#) by imrdkl (Score:2) Wednesday November 28, @04:24PM
- [Re:Uh, the answer is simple...](#) by rabidcow (Score:1) Wednesday November 28, @10:29PM
 - [Re:Uh, the answer is simple...](#) by bfree (Score:2) Thursday November 29, @10:31AM
- [Re:Uh, the answer is simple...](#) by haruharharu (Score:2) Wednesday November 28, @03:10PM
 - [Re:Uh, the answer is simple...](#) by nomadic (Score:2) Wednesday November 28, @05:37PM
 - [Re:Uh, the answer is simple...](#) by jazman_777 (Score:1) Wednesday November 28, @07:56PM
 - [Re:Uh, the answer is simple...](#) by jedidiah (Score:1) Thursday November 29, @12:54PM
 - [Re:Uh, the answer is simple...](#) by csteinle (Score:1) Wednesday November 28, @04:21PM
 - [Re:Uh, the answer is simple...](#) by green1 (Score:1) Wednesday November 28, @07:12PM
 - [Re:Uh, the answer is simple...](#) by cyril3 (Score:1) Wednesday November 28, @07:51PM
 - [Re:Uh, the answer is simple...](#) by csteinle (Score:1) Thursday November 29, @06:45AM
 - [Re:Uh, the answer is simple...](#) by seann (Score:1) Wednesday November 28, @04:42PM
 - [Re:Uh, the answer is simple...](#) by tang (Score:2) Wednesday November 28, @04:53PM
 - [Re:Uh, the answer is simple...](#) by wolf- (Score:1) Wednesday November 28, @05:40PM
 - [Re:Uh, the answer is simple...](#) by bjtuna (Score:2) Wednesday November 28, @05:55PM
 - [Re:Uh, the answer is simple...](#) by bjtuna (Score:2) Wednesday November 28, @08:43PM
 - **1 reply** beneath your current threshold.
 - **1 reply** beneath your current threshold.
 - **2 replies** beneath your current threshold.
 - [Re:Uh, the answer is simple...](#) by CaptIronfist (Score:1) Wednesday November 28, @04:09PM
 - [Re:Uh, the answer is simple...](#) by Darren Winsper (Score:1) Wednesday November 28, @04:57PM
 - [your father uses his two arms every single day?](#) by cpeterso (Score:1) Wednesday November 28, @05:16PM
 - **3 replies** beneath your current threshold.
 - [Re:Uh, the answer is simple...](#) by rnturn (Score:2) Wednesday November 28, @02:30PM
 - [Great! More programming jobs for Mac developers..](#) by SethJohnson (Score:2) Wednesday November 28, @04:01PM
 - [Re:Great! More programming jobs for Mac developers](#) by czardonic (Score:1) Wednesday November 28, @06:55PM
 - [Re:Great! More programming jobs for Mac developers](#) by innocent_white_lamb (Score:1) Wednesday November 28, @07:02PM
 - [Re:Great! More programming jobs for Mac developers](#) by czardonic (Score:1) Wednesday November 28, @08:27PM
 - [Re:Uh, the answer is simple...](#) by poot_rootbeer (Score:1) Wednesday November 28, @04:12PM
 - **2 replies** beneath your current threshold.
 - [Re:Uh, the answer is simple...](#) by n8ur (Score:2) Wednesday November 28, @01:58PM
 - [Re:Uh, the answer is simple...](#) by imrdkl (Score:1) Wednesday November 28, @04:29PM
 - [Re:Uh, the answer is simple...](#) by MojoReisen (Score:1) Wednesday November 28, @02:01PM

- [Re:Uh, the answer is simple...](#) by gazbo (Score:3) Wednesday November 28, @02:07PM
 - [Re:Uh, the answer is simple...](#) by rnturn (Score:2) Wednesday November 28, @02:34PM
 - [Re:Uh, the answer is simple...](#) by Anonymous Coed (Score:1) Wednesday November 28, @02:49PM
 - [Re:Uh, the answer is simple...](#) by ichimunki (Score:2) Wednesday November 28, @03:28PM
 - [Re:Uh, the answer is simple...](#) by LMCBoy (Score:2) Wednesday November 28, @03:51PM
 - [Re:Uh, the answer is simple...](#) by ucblockhead (Score:2) Wednesday November 28, @04:37PM
 - [Re:Uh, the answer is simple...](#) by ichimunki (Score:1) Wednesday November 28, @04:54PM
 - [Re:Uh, the answer is simple...](#) by LMCBoy (Score:2) Wednesday November 28, @05:07PM
 - [Re:Uh, the answer is simple...](#) by 179327 (Score:1) Wednesday November 28, @06:26PM
 - **1 reply beneath your current threshold.**
 - [Re:Uh, the answer is simple...](#) by blackx51 (Score:1) Wednesday November 28, @03:39PM
 - [Re:Uh, the answer is simple...](#) by rnturn (Score:2) Wednesday November 28, @04:04PM
 - **2 replies beneath your current threshold.**
 - [Except...](#) by Greyfox (Score:2) Wednesday November 28, @06:24PM
 - **1 reply beneath your current threshold.**
- [I'm a Linux user and IT IS my problem!](#) by SomethingOrOther (Score:1) Wednesday November 28, @02:11PM
- [Actually, it's even simpler...](#)

(Score:5, Interesting)

by [jd \(1658\)](#) <imipak@yahoo.com> on Wednesday November 28, @02:14PM ([#2625522](#))

(<http://slashdot.org/> | Last Journal: [Monday June 26, @02:35PM](#))

Use three intrusion detection programs, each using different cryptographic hashes, and each validating the other two.

Such an arrangement would be next to impossible to compromise, as you would need to break all three programs within the check cycle of all three of them. Either that, or you need to break all three hashing algorithms, in such a way as to find a synonym in all three key spaces. Synonyms in a single key space are going to be common, simply because you're using fewer bits. Two coinciding synonyms will be very rare, and there's no guarantee that the software could be moulded into one. THREE coinciding synonyms will be so vanishingly rare that it wouldn't be worth anyone's while to search for one that's even remotely usable.

There. Problem solved. And all it took was a bunch of Tripwire clones. And someone thought it was difficult?

[[Parent](#)]

- [Re:Actually, it's even simpler...](#) by m_evanchik (Score:2) Wednesday November 28, @02:35PM
 - **Re:Actually, it's even simpler...**

(Score:5, Informative)

by [jd \(1658\)](#) <imipak@yahoo.com> on Wednesday November 28, @03:24PM ([#2626041](#))

(<http://slashdot.org/> | Last Journal: [Monday June 26, @02:35PM](#))

This is the collection of tools I would suggest, based on what is listed on [Securityfocus](#) [securityfocus.com], for Windows 95/98 machines. Look under Windows tools. If you can't find the software on the site given as it's home, you can pick a copy up from Securityfocus.

- [Notify](#) [pc-tools.net]
- [ProtectX](#) [plasmateksoftware.com]
- [X-NetStat](#) [arez.com]

These utilities, when used together, would offer a defence, using a slightly different technique. Here, you'd be warned, the moment any intruder attempts to connect to your machine, OR your machine mysteriously attempts to connect to someone else. You also get the warning on when a file is changed.

(By relying on only one verifier, you're not quite so secure, but it was the best I could find in a short time. Apologies for that.)

[[Parent](#)]

- **1 reply beneath your current threshold.**
- [Re:Actually, it's even simpler...](#) by jd (Score:2) Wednesday November 28, @03:26PM
- **1 reply beneath your current threshold.**
- [Re:Uh, the answer is simple...](#) by drsoran (Score:1) Wednesday November 28, @04:00PM
- [Re:Uh, the answer is simple...](#) by Glorat (Score:1) Wednesday November 28, @05:13PM
- **1 reply beneath your current threshold.**
- [Re:Uh, the answer is simple...](#) by Halcyon-X (Score:1) Thursday November 29, @06:08AM
- **2 replies beneath your current threshold.**
- [Are you sure?](#) by Sc00ter (Score:3) Wednesday November 28, @01:41PM
- [Re:Are you sure?](#) by Sc00ter (Score:2) Wednesday November 28, @01:43PM
- [Re:Are you sure?](#) by dcr (Score:1) Wednesday November 28, @02:52PM
- [Re:Are you sure?](#) by Jucius Maximus (Score:1) Wednesday November 28, @03:21PM
- [Not a poke at you](#) by Archfeld (Score:2) Wednesday November 28, @04:19PM
- [Re:Not a poke at you](#) by Jucius Maximus (Score:1) Wednesday November 28, @04:49PM
- [Re:Not a poke at you](#) by Black Parrot (Score:1) Wednesday November 28, @05:45PM
- [AP Reporter Says It's Real](#) by waldoj (Score:2) Wednesday November 28, @02:02PM
- [Re:AP Reporter Says It's Real](#) by waldoj (Score:1) Wednesday November 28, @11:28PM
- **1 reply beneath your current threshold.**
- **1 reply beneath your current threshold.**
- [Nice ...](#) by BoyPlankton (Score:2) Wednesday November 28, @01:41PM
- **4 replies beneath your current threshold.**
- [So much for trusting either](#) by Archfeld (Score:2) Wednesday November 28, @01:42PM
- **1 reply beneath your current threshold.**
- [Backdoor](#) by snevine (Score:2) Wednesday November 28, @01:42PM
- [Re:Backdoor](#) by LittleGuy (Score:1) Wednesday November 28, @03:18PM
- **1 reply beneath your current threshold.**
- **1 reply beneath your current threshold.**
- [not good.....](#) by the_2nd_coming (Score:2) Wednesday November 28, @01:43PM
- [Re:not good.....](#) by zmokhtar (Score:1) Wednesday November 28, @02:05PM
- [Re:not good.....](#) by gorgon (Score:1) Wednesday November 28, @02:19PM
- [Re:not good.....](#) by zeno_2 (Score:1) Wednesday November 28, @03:03PM
- [Re:not good.....](#) by zeno_2 (Score:1) Thursday November 29, @02:25PM
- **2 replies beneath your current threshold.**
- [Re:not good.....](#) by PW2 (Score:1) Wednesday November 28, @03:02PM
- [What Credibility?](#) by Erris (Score:1) Wednesday November 28, @03:47PM
- [AC you are sorely missed.](#) by Erris (Score:1) Wednesday November 28, @10:33PM
- [Re:What Credibility?](#) by Tony-A (Score:1) Thursday November 29, @04:08AM
- **1 reply beneath your current threshold.**
- [Re:not good.....](#) by jazman_777 (Score:1) Wednesday November 28, @08:25PM
- **1 reply beneath your current threshold.**
- [opensource](#) by simpl3x (Score:2) Wednesday November 28, @01:44PM
- **1 reply beneath your current threshold.**
- **Open Source Solution?**

(Score:4, Interesting)

by boinger (4618) <boinger@fuck-yoDEGASu.org minus painter> on Wednesday November 28, @01:44PM (#2625306)

(<http://fuck-you.org/>)

How's [OpenAntiVirus](#) [sourceforge.net] doing? How does it compare to the Big Two? - If it can't hold up, do "we" have any other viable options outside of McAfee and Symantec?

- [Re:Open Source Solution?](#) by Karma 50 (Score:1) Wednesday November 28, @03:00PM
 - [Re:Open Source Solution?](#) by platypus (Score:1) Wednesday November 28, @03:24PM
 - [Re:Open Source Solution?](#) by _Sprocket_ (Score:2) Wednesday November 28, @07:28PM
- [Re:Open Source Solution?](#) by Karma 50 (Score:2) Wednesday November 28, @03:13PM
- [Use this virus scanner](#) by athmanb (Score:2) Wednesday November 28, @07:19PM
- **2 replies beneath your current threshold.**
- [Im having Deja-Vu here ...](#) by TheViffer (Score:2) Wednesday November 28, @01:44PM
 - [Re:Im having Deja-Vu here ...](#) by sheetsda (Score:2) Wednesday November 28, @02:09PM
 - [Would they pay...](#) by rnturn (Score:3) Wednesday November 28, @04:17PM
 - **1 reply beneath your current threshold.**
 - [Re:Im having Deja-Vu here ...](#) by Jedi Holocron (Score:1) Wednesday November 28, @03:50PM
 - [Grammar nitpick](#) by PurpleBob (Score:1) Wednesday November 28, @05:29PM
 - **2 replies beneath your current threshold.**
- ["Fact" Squad](#) by n-baxley (Score:1) Wednesday November 28, @01:45PM
 - [Re:"Fact" Squad](#) by n-baxley (Score:1) Wednesday November 28, @01:48PM
 - [Re:"Fact" Squad](#) by gryttype (Score:2) Wednesday November 28, @02:15PM
 - [Re:"Fact" Squad](#) by n-baxley (Score:1) Wednesday November 28, @02:37PM
- **Silly to the extreme**

(Score:5, Insightful)

by [Dark Paladin \(116525\)](#) <jhummel@johnhummel.net> on Wednesday November 28, @01:46PM (#2625314) (<http://www.theapprenticepaladin.com/>)

I'm not a conspiracy nut, and I certainly don't have total trust, or total mistrust, of the government either.

But it isn't the idea of the FBI trying to use these tools that offends me. I expect them too, and I don't have anything to hide. But the issue of a company that I pay money for to help protect me to turn a blind eye to government intrusion is insane.

If I pay someone to give me security, I expect them to provide it against anyone who wants my information. Pure and simple. And I'm not worried about the "Oh, we won't check the FBI's version - but we would check variants."

Oh, that makes me feel *much* better. Imagine a cracker getting his fingers on the FBI software and using that on my systems. Gee, thanks for *not* checking that, Symantec.

Of course, you have to admit that Symantec and McAfee are in a bind. If they state they're going to detect the FBI software, then they're anti-government. If they don't, then they're aiding big brother. But considering that the United States was formed from a healthy distrust of our government (and that distrust has only proved to help us, thank you Hubert Hoover and your bra collection), I would rather have the security companies on my side and make my government work just a little harder to prove guilt. Or at least, that's what my tax dollars should be going to.

Of course, this is just my opinion. I could be wrong.

- [Re:Silly to the extreme](#) by poot_rootbeer (Score:1) Wednesday November 28, @01:54PM
 - [Re:Silly to the extreme](#) by geomon (Score:1) Wednesday November 28, @01:56PM
- [Re:Silly to the extreme](#) by Reality Master 101 (Score:2) Wednesday November 28, @01:59PM
 - [Re:Silly to the extreme](#) by MrFredBlogs (Score:2) Wednesday November 28, @02:07PM
 - [Re:Silly to the extreme](#) by ictatha (Score:3) Wednesday November 28, @02:12PM
 - [Re:Silly to the extreme](#) by Reality Master 101 (Score:2) Wednesday November 28, @02:17PM
 - [Re:Silly to the extreme](#) by battjt (Score:1) Wednesday November 28, @02:28PM
 - [Fourth amendment](#) by jpostel (Score:2) Wednesday November 28, @04:18PM
 - **1 reply beneath your current threshold.**
 - [Re:Silly to the extreme](#) by Cro Magnon (Score:1) Wednesday November 28, @05:05PM
 - [Re:Silly to the extreme](#) by daniel_howell (Score:2) Wednesday November 28, @02:17PM
 - **1 reply beneath your current threshold.**

- [Re:Silly to the extreme](#) by bteeter (Score:1) Wednesday November 28, @02:24PM
 - [Re:Silly to the extreme](#) by monkeydo (Score:2) Wednesday November 28, @02:49PM
- [Re:Silly to the extreme](#) by Tassach (Score:2) Wednesday November 28, @02:25PM
- **Re:Silly to the extreme**

(Score:5, Insightful)

by [j7953 \(457666\)](#) on Wednesday November 28, @02:29PM ([#2625626](#))

So if you hire private security guards to protect your house, do you expect them to forcibly keep out the FBI when they have a warrant?

This analogy doesn't work because if the FBI presents a warrant I already know they're searching my house.

A more accurate analogy might be: What do you expect your security guards to do if they find out that your house is bugged? Should they not tell just because the bugs carry "FBI" labels?

[[Parent](#)]

- [Re:Silly to the extreme](#) by Cro Magnon (Score:1) Wednesday November 28, @02:37PM
- [Re:Silly to the extreme](#) by Shagg (Score:2) Wednesday November 28, @02:59PM
- [Re:Silly to the extreme](#) by bangoperator (Score:1) Wednesday November 28, @07:35PM
- [Re:Silly to the extreme](#) by FortKnox (Score:2) Wednesday November 28, @02:00PM
 - **1 reply beneath your current threshold.**
- [Re:Silly to the extreme](#) by daniel_howell (Score:1) Wednesday November 28, @02:12PM
 - [Re:Silly to the extreme](#) by jazman_777 (Score:1) Wednesday November 28, @08:33PM
- [Re:Silly to the extreme](#) by BrookHarty (Score:3) Wednesday November 28, @02:33PM
 - [Re:Silly to the extreme](#) by arglesnaf (Score:1) Wednesday November 28, @02:50PM
 - ["Position of marijuana"???](#) by poot_rootbeer (Score:1) Wednesday November 28, @04:21PM
 - [Constitution doesn't say crimes must have a victim](#) by yerricde (Score:1) Thursday November 29, @02:43AM
 - **1 reply beneath your current threshold.**
- [Re:Silly to the extreme](#) by Anonymous Coward (Score:2) Wednesday November 28, @02:34PM
- **Re:Silly to the extreme**

(Score:4, Insightful)

by [OmegaDan \(101255\)](#) on Wednesday November 28, @03:02PM ([#2625873](#))

(<http://www.monkelectric.com/>)

Once someone catches magic lantern, we're just gonna have to pay 20\$ for a magic lantern detector I already run Norton and Ad-Aware scanners, why not Lantern-Away? ... Hopefully Lavasoft (makers of ad-aware) will catch the thing and put it in their ad-aware scanner ...

I have a better conspiracy theory though ... The thing that's missing in all this is the delivery vector. *What if* norton/mcafee *are* the delivery vectors? Think about it -- they're perfect. It would prolly only add a few hundred kbytes to the program ... Virus programs automatically call home for updates (nav 2002 calls home almost every day), in one of those updates why couldn't it say "here's the newest copy of magic lantern, please install" :) And once it's in, either ML itself *or* norton anti-virus can update ML with the newest evasion techniques etc etc ...

[[Parent](#)]

- [Re:Silly to the extreme](#) by psych031337 (Score:2) Thursday November 29, @11:49AM
 - **1 reply beneath your current threshold.**
- [nothing to hide](#) by anasophist (Score:2) Wednesday November 28, @03:19PM
- [Re:Silly to the extreme](#) by yusing (Score:1) Wednesday November 28, @04:49PM
- [Cant Wait to Vote Out Bush in 2002](#) by Anonymous Coward (Score:1) Wednesday November 28, @05:35PM
 - **1 reply beneath your current threshold.**
- [Re:Silly to the extreme](#) by Vex (Score:2) Wednesday November 28, @05:38PM
- [Re:Silly to the extreme](#) by way2muchsense (Score:1) Thursday November 29, @09:35AM
- **4 replies beneath your current threshold.**

- **huh?**

(Score:5, Insightful)

by [new death barbie \(240326\)](#) on Wednesday November 28, @01:46PM ([#2625318](#))

So they're not going to detect the original, but they WILL detect any hacker-modified clones?

What about Norton Firewall? Will it still detect unexpected outgoing connections? How can I expect it to reliably detect and permit FBI-approved software, but not hacker software with a similar MO?

Oh, maybe there'll be a hard-coded IP address in the outgoing connection -- now THERE'S a nice target for DDOS!

- [Re:huh?](#) by freddie (Score:1) Wednesday November 28, @02:38PM
- [Why bother modding? Just capture the output.](#) by Tenebrious1 (Score:2) Wednesday November 28, @04:30PM
 - [PGP passphrase only? Seems unlikely.](#) by Tenebrious1 (Score:1) Thursday November 29, @01:26PM
 - **1 reply beneath your current threshold.**
- [Re:Under the current suspension of the Magna Carta](#) by Tony-A (Score:1) Thursday November 29, @02:01AM
 - **2 replies beneath your current threshold.**
- [Don't believe the hype](#) by quakeslut (Score:1) Wednesday November 28, @01:46PM
 - [Re:Don't believe the hype](#) by Happy Monkey (Score:2) Wednesday November 28, @02:38PM
 - [Re:Don't believe the hype](#) by arkanes (Score:1) Wednesday November 28, @03:04PM
 - [Re:Don't believe the hype](#) by Happy Monkey (Score:2) Wednesday November 28, @04:43PM
 - **1 reply beneath your current threshold.**
- **Great - It's a three way race**

(Score:4, Interesting)

by [Embedded Geek \(532893\)](#) on Wednesday November 28, @01:47PM ([#2625323](#))

(<http://www.thehaws.org/>)

So, now it's a three way race to see who's smarter: To see if the (1)virus writers are smart enough to make it look like their stuff is (2)FBI to (3)AV developers.

Eventually, I'm gonna need a scorecard to keep all this striaght.

- [Re:Great - It's a three way race](#) by Computer! (Score:2) Wednesday November 28, @03:07PM
 - [Hammering the FBI.](#) by Embedded Geek (Score:1) Wednesday November 28, @03:35PM
 - [Re:Great - ... Think Carnivore](#) by Knobby (Score:2) Wednesday November 28, @10:09PM
 - **1 reply beneath your current threshold.**
- [New virii](#) by mclrath (Score:2) Wednesday November 28, @01:49PM
 - [Re:New virii](#) by jjeff (Score:1) Wednesday November 28, @09:31PM
 - [Re:New virii](#) by mclrath (Score:1) Thursday November 29, @11:32AM
 - **1 reply beneath your current threshold.**
- **I can hardly wait**

(Score:5, Insightful)

by [r_j_prahad \(309298\)](#) <r_j_prahad@@@hotmail...com> on Wednesday November 28, @01:49PM ([#2625341](#))

From the time a copy of this "Magic Lantern" is first discovered in the wild until an exact copy of the FBI-approved (and consequently undetectable) version is available via alt.hackers.malicious is going to take what, twenty minutes?

Malda might as well start composing (and spellchecking) the headline now, because it's a sure bet he'll get to use it.

- [Re:I can hardly wait](#) by KernelHappy (Score:2) Wednesday November 28, @02:43PM
 - **Savvy**

(Score:5, Interesting)

by [ucblockhead \(63650\)](#) on Wednesday November 28, @03:09PM ([#2625928](#))

(<http://www.ucblockhead.org/journal/> | Last Journal: [Thursday November 14, @04:24PM](#))

It likely won't be long before someone writes something that automatically detects the attempt to install "Magic Lantern" and then turns on a "Magic Lantern" emulator that sends exactly whatever keystrokes

the crook wants sent. Imagine the fun that could be had... A nasty crook could have fun implicating all sorts of innocent people in criminal activities.

[[Parent](#)]

- [Re:Savvy](#) by linzeal (Score:1) Wednesday November 28, @05:26PM
 - [Re:Savvy](#) by ucblockhead (Score:2) Wednesday November 28, @06:22PM
 - [Re:Savvy](#) by linzeal (Score:1) Wednesday November 28, @11:02PM
- **Ten minutes, tops.**

(Score:5, Funny)

by [roystgnr \(4015\)](#) <roystgnr@NoSPaM.ticam.utexas.edu> on Wednesday November 28, @04:32PM (#2626516)

(<http://slashdot.org/>)

What does the FBI need to do to keep American computers secure from terrorists?

Keep "Magic Lantern" out of the hands of criminals.

How does "Magic Lantern" work?

The FBI sends it to criminals.

[[Parent](#)]

- **1 reply beneath your current threshold.**
- [Re:I can hardly wait](#) by KarmaBlackballed (Score:2) Wednesday November 28, @04:33PM
- **1 reply beneath your current threshold.**
- [Legal problems for anti-virus companies ?](#) by Krapangor (Score:1) Wednesday November 28, @01:49PM
 - [Re:Legal problems for anti-virus companies ?](#) by czardonic (Score:1) Wednesday November 28, @02:01PM
 - [Re:Legal problems for anti-virus companies ?](#) by KernelHappy (Score:2) Wednesday November 28, @03:07PM
 - **2 replies beneath your current threshold.**
- [What if...](#) by COBOL/MVS (Score:2) Wednesday November 28, @01:49PM
 - **1 reply beneath your current threshold.**
- [bah](#) by mikedotd (Score:1) Wednesday November 28, @01:51PM
- [Is this any real suprise?](#) by jaseuk (Score:2) Wednesday November 28, @01:51PM
 - [Re:Is this any real suprise?](#) by czardonic (Score:2) Wednesday November 28, @02:08PM
 - [Re:Is this any real suprise?](#) by jaseuk (Score:1) Thursday November 29, @09:39AM
- [One URL says it all...](#) by MsGeek (Score:2) Wednesday November 28, @01:51PM
 - [Very true ..](#) by TheViffer (Score:1) Wednesday November 28, @02:00PM
 - [Re:Very true ..](#) by cez (Score:1) Wednesday November 28, @02:33PM
 - [My bad ...](#) by TheViffer (Score:1) Wednesday November 28, @02:48PM
 - [But F-PROT is a virus! \(According to Symantec\)](#) by Ktistec Machine (Score:1) Wednesday November 28, @02:04PM
- **Re: a/v software**

(Score:5, Insightful)

by [blibbleblobble \(526872\)](#) on Wednesday November 28, @01:52PM (#2625358)

The FBI? Do anything illegal? Who would ever imagine that such a thing could happen?

<repressed_memory>

- Wiretaps of opposition politicians
- Wiretaps of civil rights protestors
- Wiretaps of those who voice dissent
- Wiretaps of people unrelated to any crime investigation

</repressed_memory>

Hmmm, I can't seem to think of any examples of how police spy powers have been abused in the past, can you?

- [Re: a/v software](#) by the Man in Black (Score:3) Wednesday November 28, @02:06PM
 - [Re: a/v software](#) by blair1q (Score:2) Wednesday November 28, @02:18PM
 - **1 reply beneath your current threshold.**
 - [Re: a/v software](#) by imrdkl (Score:1) Wednesday November 28, @04:15PM
 - [Re: a/v software](#) by linzeal (Score:2) Wednesday November 28, @05:28PM
 - [I smell a Political Platform!](#) by Anarchofascist (Score:1) Thursday November 29, @01:37PM
- [Re: a/v software](#) by agbert (Score:1) Wednesday November 28, @07:59PM
- **1 reply beneath your current threshold.**
- **Reverse engineers line up here -**

(Score:4, Interesting)

by [Medievalist \(16032\)](#) on Wednesday November 28, @01:52PM ([#2625361](#))

Well, if the antivirus vendors are going to include a sufficiently detailed signature in their products for the FBI's virii, that should help anyone trying to build a detector.

I'm sure somebody will try to build malware that impersonates this so-called "Magic Lantern" - I hope they call it "Magic Latrine" :^).

But wouldn't it be nice to see a GPL'd program to detect the FBI's virus? Then, if I found it on my machine, I could stop the government-sponsored theft of my CPU cycles. Of course, I'd then call the FBI and offer to let them reinstall it given adequate monetary compensation - but that's just me, you might take some other action.

--Charlie

- [Re:Reverse engineers line up here -](#) by Procrasti (Score:1) Wednesday November 28, @02:22PM
 - [Re:Reverse engineers line up here -](#) by Medievalist (Score:1) Wednesday November 28, @02:52PM
 - **1 reply beneath your current threshold.**
 - [Re:Reverse engineers line up here -](#) by Procrasti (Score:1) Thursday November 29, @07:05AM
 - **1 reply beneath your current threshold.**
- **2 replies beneath your current threshold.**
- [Modding the Defs](#) by thryllkill (Score:1) Wednesday November 28, @01:52PM
- [the other guy](#) by Capt Dan (Score:1) Wednesday November 28, @01:54PM
- **J. Edgar Hoover lives on...**

(Score:4, Interesting)

by [coolgeek \(140561\)](#) on Wednesday November 28, @01:55PM ([#2625381](#))

(<http://slashdot.org/>)

Sorry for the -dash- of a conspiracy theory here, but I really wonder what the spooks have on these guys. The thought that McAfee, Symantec, et.al. could be implicated for obstructing an investigation is absurd. Well, maybe not with John Ashcroft-Hitler running the DoJ. Anyway, back to my point. Here's an opinion from a judge who upheld a citizens' right to use a radar detector:

*If government seeks to use clandestine and furtive methods to monitor citizen actions, it can ill afford to complain should the citizen insist on a method to effect his right to know he is under such surveillance.
Judge Joseph Ryan, Superior Court, District of Columbia*

Granted, its only a district court, however it is a compelling opinion, and a brilliant interpretation of the Fourth Amendment. IR detection/imaging and monitoring utility bills have been tossed out on similar grounds. I wonder what AVP is going to choose... Perhaps this is a great opportunity for Free Software, I just wonder how a free software anti-virus lab would work. Anyway, end of my rant.

- [Re:J. Edgar Hoover lives on...](#) by rho (Score:1) Wednesday November 28, @02:29PM
 - [Re:J. Edgar Hoover lives on...](#) by 3am (Score:2) Wednesday November 28, @02:34PM

If US software companies want to sell crippleware in the interests of "patriotism" that's their business. There are plenty of companies willing to fill the gap.

- o [Re:just say no](#) by zericm (Score:1) Wednesday November 28, @02:41PM
 - [Re:just say no](#) by killmenow (Score:1) Wednesday November 28, @03:40PM
 - o [beginning of end for US- based antivirus software](#) by poopie (Score:2) Wednesday November 28, @07:15PM
- **What about KGB/Mossad/MI6 trojans?**

(Score:4, Funny)

by [ENOENT \(25325\)](#) on Wednesday November 28, @01:57PM ([#2625395](#))

(<http://slashdot.org/> | Last Journal: [Thursday August 07, @03:38PM](#))

Will Symantec also ignore trojans produced by other nations' intelligence agencies? Someone should encourage some third-world countries to set up online membership signups for their intelligence agencies at a nominal fee. Crackers will then be able to continue to do what they do without breaking any laws.

- o [Re:What about KGB/Mossad/MI6 trojans?](#) by Kengineer (Score:1) Wednesday November 28, @02:15PM
- [Open Source Virus Detector?](#) by cheese_wallet (Score:1) Wednesday November 28, @01:57PM
- [Only the FBI's programs?](#) by Kissing Crimson (Score:1) Wednesday November 28, @01:59PM
- o [Re:Only the FBI's programs?](#) by malarkey (Score:1) Wednesday November 28, @02:28PM
- [Why would the FBI do this?](#) by jhubbard (Score:1) Wednesday November 28, @01:59PM
- o [Re:Why would the FBI do this?](#) by quinto2000 (Score:1) Wednesday November 28, @02:33PM
 - o **2 replies beneath your current threshold.**
- **Stance of non-us companies?**

(Score:4, Interesting)

by [Splat \(9175\)](#) on Wednesday November 28, @02:00PM ([#2625416](#))

Does anyone know the stance of non-US companies of anti-virus software on Magic Lantern? If a foreign product detects an FBI trojan horse will it then become illegal under some US law?

- o [Re:Stance of non-us companies?](#) by t_allardyce (Score:1) Wednesday November 28, @02:12PM
- **possible detection still exists**

(Score:4, Informative)

by [jeffy124 \(453342\)](#) on Wednesday November 28, @02:00PM ([#2625417](#))

(<http://slashdot.org/my/amigos> | Last Journal: [Sunday July 25, @03:59PM](#))

most AV tools (including Symantec and McAfee) monitor program execution for anomolis behavior by unknown virii. would lantern be able to avoid being detected by that?

also, what about personal firewall programs? I use a Tiny Software's PF (yes, under Windows, sad isnt it) that checks the md5 of an executable before granting internet access. on top of that, it can allow you to block certain apps from making/accepting connections from various sites. for example I have it set to not allow Mozilla access to ads.x10.com.

Here, two things exist: the lantern has to find a way around the md5 and also find a way around "PGP wants to connect to [fbi-ip-address], allow it?" Getting through one or the other might prove difficult.

- [cut out the middle man](#) by technoCon (Score:2) Wednesday November 28, @02:01PM
 - o **1 reply beneath your current threshold.**
 - [Security through Obscurity and Windows.](#) by thesolo (Score:2) Wednesday November 28, @02:02PM
 - o [chant](#) by Tony-A (Score:1) Thursday November 29, @04:33AM
 - o **1 reply beneath your current threshold.**
 - [OK This bugs me.](#) by Red Weasel (Score:1) Wednesday November 28, @02:02PM
 - o **1 reply beneath your current threshold.**
 - [Lead by example](#) by fishebulb (Score:1) Wednesday November 28, @02:03PM
 - [Press Coverage](#) by scott1853 (Score:2) Wednesday November 28, @02:03PM
 - [Cmon guys! Give me a break.](#) by Newer Guy (Score:1) Wednesday November 28, @02:04PM
 - [Recording keystrokes](#) by ehiris (Score:1) Wednesday November 28, @02:04PM
 - o **1 reply beneath your current threshold.**
 - [No way to misuse this?](#) by bahtama (Score:1) Wednesday November 28, @02:05PM
- **international terrorist: fbi**

(Score:5, Insightful)

by [SubtleNuance \(184325\)](#) on Wednesday November 28, @02:06PM ([#2625467](#))

(Last Journal: [Thursday November 28, @10:21AM](#))

How long until this little app ends up on a PC that is not on US soil? Will some foreign nation be able to make an official-issue of this? It seems like the FBI might not be thinking this through.

... then again, there is [Echelon](#) [[echelonwatch.org](#)].... apparently no one minds...

- [Re:international terrorist: fbi](#) by imrdkl (Score:1) Wednesday November 28, @02:31PM
- [international incident](#) by zoombat (Score:1) Wednesday November 28, @02:54PM
- [Re:against NAI](#) by karji (Score:1) Wednesday November 28, @06:17PM
- [It's so nice being an American.](#) by glrotate (Score:1) Wednesday November 28, @03:52PM
 - [Re:It's so nice being an American.](#) by seann (Score:1) Wednesday November 28, @05:20PM
 - **1 reply beneath your current threshold.**
- **1 reply beneath your current threshold.**
- **The funny part...**

(Score:4, Interesting)

by [Lumpy \(12016\)](#) on Wednesday November 28, @02:07PM ([#2625471](#))

(<http://timgray.blogspot.com/>)

This will only catch the dumb or the pedophiles.

Are they writing this "virus" for BeOS? how about OS/2?

What about a linux box running as only old a.out?

I can think of at least 70 ways to make their "virus" not work on my machine. (I highly doubt that this "virus" will run on my Linux development box that uses a Hitachi SH4 processor)

all this hubub about company X or software Z will or will not detect this virus app is pure marketing and hype. Noone who is really threatened by this could care as it is easily defeated from ever infecting the system by simply changing the archetecture..... Hey FBI, not everyone runs windows on Intel hardware.

- [Re:The funny part...](#) by Snowfox (Score:1) Wednesday November 28, @02:42PM
 - [Dreamcast has SH4](#) by yerricde (Score:1) Thursday November 29, @12:55AM
- [Re:The funny part...](#) by jeorgen (Score:1) Wednesday November 28, @02:56PM
- [Re:The funny part...](#) by BitterOak (Score:1) Wednesday November 28, @03:30PM
 - [Re:The funny part...](#) by PurpleBob (Score:2) Wednesday November 28, @05:07PM
 - [Re:The funny part...](#) by BitterOak (Score:1) Wednesday November 28, @07:16PM
 - [Re:The funny part...](#) by Lumpy (Score:2) Wednesday November 28, @09:24PM
- [Re:The funny part...](#) by ryanvm (Score:2) Wednesday November 28, @03:32PM
 - [Re:The funny part...](#) by Lumpy (Score:2) Wednesday November 28, @09:19PM
- **2 replies beneath your current threshold.**
- [Hmm...](#) by drift factor (Score:3) Wednesday November 28, @02:07PM
 - [Re:Hmm...](#) by blair1q (Score:1) Wednesday November 28, @02:16PM
 - [Re:Hmm...](#) by pj7 (Score:1) Wednesday November 28, @02:20PM
 - [Re:Hmm...](#) by rnturn (Score:2) Wednesday November 28, @05:09PM
 - [Re:Hmm...](#) by Karma 50 (Score:1) Wednesday November 28, @02:34PM
 - [Re:Hmm...](#) by baptiste (Score:2) Wednesday November 28, @05:30PM
- [Run Your Own with MD5 Checksums / or follow IRQs](#) by teambps (Score:1) Wednesday November 28, @02:07PM
- [Doesn't AV software..](#) by Mournblade (Score:1) Wednesday November 28, @02:09PM
- [look.](#) by gnurd (Score:1) Wednesday November 28, @02:09PM
- [As if....](#) by pj7 (Score:1) Wednesday November 28, @02:09PM
 - [Re:As if....](#) by m_evanchik (Score:2) Wednesday November 28, @02:31PM
 - **1 reply beneath your current threshold.**
- [is zonealram going to follow ?](#) by hack0rama (Score:1) Wednesday November 28, @02:10PM
 - **2 replies beneath your current threshold.**
- [Echo Effect](#) by CDWert (Score:1) Wednesday November 28, @02:10PM

- [Nothing new here.](#) by zulux (Score:1) Wednesday November 28, @02:11PM
- [tell symantec how you feel](#) by spamspam (Score:1) Wednesday November 28, @02:13PM
- [Thanks to Ashcroft](#) by NineNine (Score:1) Wednesday November 28, @02:13PM
 - **2 replies beneath your current threshold.**
- [Clairvoyant Virus Detection](#) by Zanguinar (Score:1) Wednesday November 28, @02:14PM
- [A new market](#) by actappan (Score:1) Wednesday November 28, @02:15PM
- [I am not an American!](#) by cyba (Score:2) Wednesday November 28, @02:16PM
 - [I dont trust the European Government either..](#) by Quazion (Score:1) Wednesday November 28, @02:20PM
 - [It's only for later reference](#) by tinkerton (Score:1) Wednesday November 28, @07:22PM
- [Who needs 3rd party software?](#) by crimoid (Score:3) Wednesday November 28, @02:16PM
- [Symantec may not...](#) by tweakt (Score:1) Wednesday November 28, @02:18PM
 - [Re:Symantec may not...](#) by JatTDB (Score:2) Wednesday November 28, @02:37PM
- [2 Points](#) by dbretton (Score:1) Wednesday November 28, @02:21PM
- [If I had a dime...](#) by Merlin_ (Score:1) Wednesday November 28, @02:21PM
- [Couldn't Someone Else Write A Detection Tool?](#) by ras_b (Score:1) Wednesday November 28, @02:22PM
- [Someone help me figure this one out..?](#) by linuxrunner (Score:3) Wednesday November 28, @02:23PM
 - [Re:Someone help me figure this one out..?](#) by jjeff (Score:1) Wednesday November 28, @09:20PM
 - [Re:Someone help me figure this one out..?](#) by rabidcow (Score:1) Wednesday November 28, @10:39PM
- [This will only hurt legitimate customers.](#) by thesolo (Score:1) Wednesday November 28, @02:23PM
- [I wonder if we're not hearing...](#) by kingpin2k (Score:1) Wednesday November 28, @02:23PM
 - [Re:I wonder if we're not hearing...](#) by smack_attack (Score:1) Wednesday November 28, @03:39PM
- [Who does this stop?](#) by rootmonkey (Score:1) Wednesday November 28, @02:24PM
- [A flawed concept](#) by TheoFish (Score:2) Wednesday November 28, @02:24PM
- [Developing? May already exist.](#) by uslinux.net (Score:2) Wednesday November 28, @02:25PM
 - [well, check this weeks hot virus](#) by tinkerton (Score:1) Wednesday November 28, @07:47PM
- [What about the rest of the world....](#) by someguyintoronto (Score:1) Wednesday November 28, @02:27PM
- [Buy an antivirus written outside US \(like AVP\)](#) by melted (Score:1) Wednesday November 28, @02:29PM
- [Oppertunity for Anti-Virus software vendors...](#) by WndrBr3d (Score:1) Wednesday November 28, @02:29PM
- [General comments](#) by Matrix12 (Score:1) Wednesday November 28, @02:30PM
- [Um, what was that again?](#) by LittleGuy (Score:1) Wednesday November 28, @02:31PM
- [Your tax dollars at work](#) by GrumpyOldManager (Score:1) Wednesday November 28, @02:31PM
- [I am in Canada A](#) by VEGETA_GT (Score:2) Wednesday November 28, @02:31PM
- [non-US AV software](#) by Anonymous Coward (Score:1) Wednesday November 28, @02:31PM
- [Like encryption debate?](#) by zoombat (Score:1) Wednesday November 28, @02:32PM
- [Alternate AntiVirus vendors?](#) by baglunch (Score:1) Wednesday November 28, @02:32PM
- [Boycot](#) by jfroot (Score:1) Wednesday November 28, @02:36PM
- [Will Symantec pay me back](#) by famazza (Score:2) Wednesday November 28, @02:37PM
- [What happens...](#) by Nickodemus (Score:1) Wednesday November 28, @02:38PM
- **Not these company's job anyway**

(Score:5, Insightful)

by [iabervon \(1971\)](#) on Wednesday November 28, @02:43PM (#2625733)

(<http://iabervon.org/~barkalow/> | Last Journal: [Saturday May 31, @03:01AM](#))

These companies provide detection and removal services for widely-distributed and automatic attacks. That is to say, it's their job to clean up when someone releases a virus that spreads all over the place. They discover something spreading, and they make an update.

If the FBI is doing their job well, that's not the situation here. The way they've been describing this working is that they set it up to attack the particular person against whom they've obtained a warrant. It doesn't email itself to the target's addressbook, it doesn't attack random IPs, it doesn't try to infect floppies. That would be both illegal (since it could destroy the data of non-targets) and probably invalidate their evidence (since they don't have a warrant to investigate every individual in the US).

So a virus scanner shouldn't catch Magic Lantern, because it's not really a virus, in the sense that they're scanning for. It's an attack tool, which uses the methods often employed by viruses. Virus scanners don't fix security holes; they look for particular malicious and spreading code on your computer and clean it up. They won't stop Magic Lantern, they won't stop someone hijacking your passport account, and they won't stop even script kiddies breaking into your webserver, because their purpose and system design just aren't good for that.

So far I haven't heard of any IDS companies saying they will ignore ML, nor have I heard of any companies saying they won't fix security holes that ML uses. That's what would be significant.

- [Re:Not these company's job anyway](#) by scaryjohn (Score:1) Wednesday November 28, @05:37PM
 - [Re:Not these company's job anyway](#) by iabervon (Score:2) Friday November 30, @12:30AM
- [Re:Not these company's job anyway](#) by david.johns (Score:1) Wednesday November 28, @07:18PM
- [Is Magic Lantern a virus](#) by dkh (Score:1) Wednesday November 28, @02:43PM
 - [Re:Is Magic Lantern a virus](#) by Knobby (Score:2) Wednesday November 28, @03:59PM
- [Why this does not bother me](#) by drix (Score:2) Wednesday November 28, @02:45PM
- [Vaccanation idea...](#) by AtariDatacenter (Score:1) Wednesday November 28, @02:48PM
- [magic lattern will get DDOSed](#) by Twillerror (Score:2) Wednesday November 28, @02:50PM
- [What I don't get...](#) by jabber01 (Score:3) Wednesday November 28, @02:50PM
 - [Re:What I don't get...](#) by Black Parrot (Score:2) Wednesday November 28, @05:36PM
 - [Re:What I don't get...](#) by matrix29 (Score:1) Wednesday November 28, @09:11PM
 - [Re:What I don't get...](#) by Lord Omlette (Score:2) Wednesday November 28, @10:39PM
- [Its Called VIRUS detection after all](#) by joshv (Score:2) Wednesday November 28, @02:52PM
 - [Re:Its Called VIRUS detection after all](#) by tinkerton (Score:1) Wednesday November 28, @07:14PM
- [Bunch of bs....](#) by MarkCollins (Score:1) Wednesday November 28, @02:54PM
- [This is getting bad...](#) by nochops (Score:1) Wednesday November 28, @02:56PM
 - [Re:This is getting bad...](#) by nochops (Score:1) Wednesday November 28, @04:15PM
 - **1 reply beneath your current threshold.**
- [sue them..](#) by Suppafly (Score:1) Wednesday November 28, @02:58PM
- [How are they going to install this?](#) by joshv (Score:2) Wednesday November 28, @03:05PM
 - [Re:How are they going to install this?](#) by linuxrunner (Score:2) Wednesday November 28, @04:17PM
 - [Re:How are they going to install this?](#) by joshv (Score:1) Wednesday November 28, @04:37PM
 - [Re:How are they going to install this?](#) by jjeff (Score:1) Wednesday November 28, @09:52PM
 - **1 reply beneath your current threshold.**
- [NEWS FLASH](#) by DarkZero (Score:2) Wednesday November 28, @03:06PM
- [I can just see the headlines](#) by raptor21 (Score:1) Wednesday November 28, @03:07PM
- [Dismantle the US government NOW!](#) by The Man (Score:2) Wednesday November 28, @03:08PM
 - **1 reply beneath your current threshold.**
- [fraud?](#) by Deadplant (Score:2) Wednesday November 28, @03:14PM
- [I, for one, am pleased!](#) by Xaroth (Score:1) Wednesday November 28, @03:14PM
- [Boycott Proselytism](#) by Narril Duskwalker (Score:1) Wednesday November 28, @03:15PM
- [NAI - Symantec, firewalls and PGP](#) by Anonymous Coward (Score:1) Wednesday November 28, @03:17PM
- [Is that just as bad?](#) by C_Mattie (Score:1) Wednesday November 28, @03:17PM
- [When I buy a new lock....](#) by arson1 (Score:1) Wednesday November 28, @03:18PM
 - [Re:When I buy a new lock....](#) by GrumpyOldManager (Score:1) Wednesday November 28, @03:31PM
- [looks like...](#) by giantsquidmarks (Score:1) Wednesday November 28, @03:20PM
- [details details](#) by Deadplant (Score:1) Wednesday November 28, @03:35PM
- [Another one?](#) by Shelle (Score:1) Wednesday November 28, @03:35PM
- [FBI information](#) by Nemith (Score:1) Wednesday November 28, @03:37PM
- [US AV companies can now disappear](#) by aliebrah (Score:2) Wednesday November 28, @03:39PM
 - [open market for better AV's?](#) by tinkerton (Score:1) Wednesday November 28, @06:56PM
 - **1 reply beneath your current threshold.**
- [hmmm whats this....](#) by Pyrosz (Score:1) Wednesday November 28, @03:40PM
- [DOS on Magic Lantern](#) by Embedded Geek (Score:2) Wednesday November 28, @03:40PM
- **Could Magic Lantern be buit into Windows XP**

(Score:5, Insightful)

by [savaget \(26702\)](#) on Wednesday November 28, @03:51PM ([#2626208](#))

Would it be possible for Magic Lantern to be built into a closed source OS like Windows XP?

- **Re:Could Magic Lantern be buit into Windows XP**

(Score:5, Informative)

by [Embedded Geek \(532893\)](#) on Wednesday November 28, @04:03PM ([#2626294](#))

(<http://www.thehaws.org/>)

I guess it could. From an engineering standpoint it would make more sense. The FBI need merely turn it on,

not infect/install it themselves. If MS threw this bone to the DOJ, they might consider some quid pro quo on the antitrust front (not like they need to with the way things are going, though).

'Hadn't thought of that option before. Of course, I will now. Probably not get any sleep for a few days, too.

[[Parent](#)]

- [Re:Could Magic Lantern be buit into Windows XP](#) by Black Parrot (Score:2) Wednesday November 28, @05:40PM
- [Linux -- the choice of discriminating evil doers](#) by iskander (Score:1) Thursday November 29, @01:35AM
- [Re:Could Magic Lantern be buit into Windows XP](#) by Tony-A (Score:1) Thursday November 29, @02:34AM
- **1 reply beneath your current threshold.**
- [Re:Could Magic Lantern be buit into Windows XP](#) by Pinball Wizard (Score:1) Wednesday November 28, @04:13PM
- [Re:Could Magic Lantern be buit into Windows XP](#) by Baba Abhui (Score:1) Wednesday November 28, @04:44PM
 - [Re:Could Magic Lantern be buit into Windows XP](#) by dstone (Score:3) Wednesday November 28, @05:02PM
 - [Re:Could Magic Lantern be buit into Windows XP](#) by acceleriter (Score:1) Wednesday November 28, @06:14PM
 - [simpler](#) by tinkerton (Score:1) Wednesday November 28, @07:10PM
 - [Re:Could Magic Lantern be buit into Windows XP](#) by dstone (Score:2) Wednesday November 28, @07:12PM
 - [Re:Could Magic Lantern be buit into Windows XP](#) by Lagged2Death (Score:1) Wednesday November 28, @09:03PM
- [Re:Could Magic Lantern be buit into Windows XP](#) by ShogZilla (Score:1) Wednesday November 28, @06:42PM
 - [Re:Could Magic Lantern be buit into Windows XP](#) by GraLab (Score:1) Thursday November 29, @12:35AM
- [Re:Could Magic Lantern be buit into Windows XP](#) by Sloppy (Score:1) Thursday November 29, @12:54AM
- [Re:Could Magic Lantern be buit into Windows XP](#) by babbage (Score:2) Thursday November 29, @11:50AM
- **1 reply beneath your current threshold.**
- [B.S.](#) by rice_burners_suck (Score:2) Wednesday November 28, @03:53PM
- [wrong focus](#) by elmegil (Score:2) Wednesday November 28, @03:53PM
- [Just a thought..](#) by Coleco (Score:1) Wednesday November 28, @03:55PM
- [Legal in other countries?](#) by sammy.lost-angel.com (Score:1) Wednesday November 28, @03:55PM
- [Biometrics?](#) by senseimoron (Score:1) Wednesday November 28, @04:03PM
 - [Re:Biometrics?](#) by Junta (Score:2) Wednesday November 28, @04:49PM
- [What would prevent hackers..](#) by Axe (Score:1) Wednesday November 28, @04:05PM
- [Fed -B-Gone v0.34beta](#) by greygent (Score:1) Wednesday November 28, @04:10PM
- [Ehehehe, Bad idea, Bad bad bad](#) by Delifisek (Score:1) Wednesday November 28, @04:12PM
- [Implications](#) by Hoo00 (Score:1) Wednesday November 28, @04:16PM
 - [Re:Implications](#) by daveman_1 (Score:1) Wednesday November 28, @05:41PM
- [maybe ad-aware can take care of this](#) by Indy1 (Score:1) Wednesday November 28, @04:28PM
- [Huh?](#) by exceed (Score:1) Wednesday November 28, @04:31PM
- [Can't wait for the lawsuits.](#) by KingBozo (Score:1) Wednesday November 28, @04:36PM
 - [You must have forgotten the "USA" Terrorism Bill](#) by eclectic (Score:1) Wednesday November 28, @05:30PM
- [I use AVG by Grisoft...](#) by Kalabajoui (Score:2) Wednesday November 28, @04:47PM
- [Norton AV](#) by Spiffy (Score:1) Wednesday November 28, @04:59PM
- [Zone Alarm?](#) by spoonyfork (Score:2) Wednesday November 28, @05:11PM
- [FBI/Hackers, same thing.](#) by neoevans (Score:1) Wednesday November 28, @05:33PM
- [boycott](#) by samantha (Score:2) Wednesday November 28, @05:35PM
- [Free AV](#) by CrashRide (Score:1) Wednesday November 28, @05:53PM
- [Magic Lantern Honey Pot?](#) by wytld (Score:2) Wednesday November 28, @05:54PM
- [Tripwire](#) by silversurf (Score:1) Wednesday November 28, @06:04PM

- [Symantec Customer Service not on the same page!](#) by The_THOMAS (Score:1) Wednesday November 28, @06:12PM
- [Slippery slope](#) by Simon Garlick (Score:1) Wednesday November 28, @06:25PM
- [The truth](#) by shag_and_scooby_too (Score:1) Wednesday November 28, @06:53PM
- ["However we would detect modified versions"](#) by Honest Man (Score:1) Wednesday November 28, @07:17PM
- [Why does it matter?](#) by de_boer_man (Score:1) Wednesday November 28, @07:23PM
- [Think about this angle.](#) by Archangel Michael (Score:2) Wednesday November 28, @07:59PM
- [KeyKatcher a consumer solution to keystroking](#) by gman13 (Score:1) Wednesday November 28, @08:03PM
- [immigrants](#) by staeci (Score:1) Wednesday November 28, @09:14PM
- [the real conspiracy](#) by staeci (Score:1) Wednesday November 28, @09:25PM
- [ECHELON.](#) by Cinematique (Score:1) Wednesday November 28, @10:18PM
- [And the point of all this...](#) by Cosmic Cow (Score:1) Wednesday November 28, @10:43PM
- [Why are they announcing this to the public](#) by RodeoBoy (Score:1) Thursday November 29, @12:09AM
- [Already recommended against McAfee](#) by matttr (Score:2) Thursday November 29, @02:44AM
- [Magic Lantern and you.](#) by AftanGustur (Score:2) Thursday November 29, @07:36AM
- [Re:3rd party AV](#) by bigpat (Score:1) Wednesday November 28, @01:53PM
 - [Re:3rd party AV](#) by Stonehand (Score:1) Wednesday November 28, @02:05PM
 - [Re:3rd party AV](#) by bigpat (Score:1) Friday November 30, @05:09PM
 - **1 reply beneath your current threshold.**
- [Re:3rd party AV](#) by crankyspice (Score:1) Wednesday November 28, @02:08PM
- [Re:Why Does This Surprise Anyone???](#) by jeffphil (Score:1) Wednesday November 28, @02:23PM
- [Re:I run linux blah blah blah!!!](#) by Todd Knarr (Score:2) Wednesday November 28, @02:40PM
- [Re:Magic Lantern & Medical Marijuana](#) by daveman_1 (Score:1) Wednesday November 28, @05:36PM
 - **1 reply beneath your current threshold.**
- **34 replies beneath your current threshold.**
-

(1) | 2

Immature poets imitate, mature poets steal. -- T.S. Eliot, "Philip Massinger"

All trademarks and copyrights on this page are owned by their respective owners. Comments are owned by the Poster. The Rest © 1997-2007 [OSTG](#).