

www.futurebrief.com

Terror-Bytes...

Jeffrey R. Harrow
Principal Technologist, The Harrow Group

You (or someone you designate) probably (hopefully) spends a fair amount of time worrying about the viruses and worms and adware and malware that terrorize our PCs. It's definitely worth musing about this for both your home and your business, given that these terror-bytes do hold the very real, all-to-often demonstrated threat of compromising the privacy and security of your personal and business information.

(Protection Overview: Without going into detail here, *EVERY* PC should, at a minimum, implement these defenses: a software firewall such as ZoneAlarm; a good antivirus program that is automatically updated on a frequent schedule such as AVG Anti-Virus; and one or more programs to identify and remove adware and malware such as AdAware and Spybot Search and Destroy. Without such a multi-layered defensive screen you are truly at risk. How much at risk? If you connect a newly-minted Windows XP PC to the Internet and DO NOTHING, the average time-to-infection has been measured at 16 minutes!)

I'll call these and similar assaults "electronic terrorism."

But there's far more at stake here than just individual PCs.

Law Enforcement As Target.

In a Dec. 8, 2005 CNN.com [article](#), FBI Assistant Director Louis Reigle, the head of their Cyber Division, stated that,

"There's nothing on my desk today or the director's desk that would cause any concern today."

In that same vein, FBI Computer Intrusion head Peter Trahon states that,

"We're not aware of any plan to attack U.S. infrastructure."

Assuming their intelligence is correct (and I have no reason to suggest otherwise), I believe that it certainly remains feasible for Internet-based "warfare" to either engage in an economic attack on a country, or to complicate more conventional warfare. Even if an attacker could not gain direct access to the target country's critical civilian or military infrastructure, imagine if an electronic attack "only" disabled a country's segments of the Internet and their business and personal PCs. Even such an indirect attack could, in effect, bring a country to its economic knees.

(By way of an "indirect" infrastructure attack, consider that the Sober computer worm recently sent out a vast number of SPAM emails. They were doctored so that their "From" address was that of the FBI (although that was not the case.) When these bogus messages then hit the Internet mail servers of the millions of random recipients (most of which did not represent valid Email accounts), those mail servers (correctly) "bounced" a message back to the *assumed* sender - in this case the FBI.

www.futurebrief.com

The FBI Email servers received over 200,000 "bounce" messages per hour which, according to Reigel, "...almost killed our system." Note that it's already been demonstrated, too many times, that Email and Web servers can indeed be brought to their virtual knees through various Internet-based attacks.)

While I have to believe that the FBI's public Email server is not a mission-critical component of their law enforcement operations, I also have to believe that in this age of the pervasive use of Email, law enforcement agencies, like businesses, have become increasingly dependent on public Email for much of their non-internal/non-critical business. Similarly, especially poignant around the holiday season when many retail businesses make a significant percentage of their annual sales, a disruption of their online divisions' shopping systems could make a serious economic dent in their bottom lines, and hence in the GNP.

Such issues deserve careful study and appropriate protections.

But on a somewhat lighter note, it's not just traditional Internet-based servers and services that are at risk.

Entertainment Terrorism.

Consider, for example, a new product that "fights with light" to attack local TV sets!



Called the "[TV-B-Gone](#)", this car-remote-control sized "fob" has a single button. When pushed, it rapidly beams out the various infrared light codes, one right after another, that [cause most TVs to turn themselves off!](#)

TVs in bars, store windows, classrooms, kiosks, businesses, in fact in virtually any setting, can now be easily silenced with no one being the wiser as to who is perpetrating this public entertainment terrorism.

This ability to control various infrared devices is hardly new -- anyone seriously interested in affecting a particular TV only needs to purchase an inexpensive "universal" remote control that can be programmed on the fly to work with a given TV. There are also programs that will turn a PDA into a remote. There are even wristwatches costing as little as \$30, such as the [Midas](#), that provide similar universal remote capabilities.



Happily, most of these devices work with one TV's codes at a time; they don't send out every model's "turn-off" codes at once like the TV-B-Gone.

There are certainly times when I'd appreciate having a disruptive TV turned off, but as with other forms of vigilantism, a TV Turn Off device could easily result in entertainment chaos.

The Broader Issue Is NOT Trivial!

Silencing TVs may seem to be (and usually is) a trivial issue in the grand scheme of things. But if we look forward to a time when virtually everything might be remotely controllable, either locally via infrared or radio signals, or over the Internet (as is already the case for TiVo digital video recorders, some home security systems, and far more), then enhanced forms of electronic terrorism might expand in some very uncomfortable directions.

Today, a small piece of opaque tape placed over a TV remote control receiver window will cure the problem (although it will also prevent legitimate remote control by its owner). But this countermeasure will not be so simple in the future.

Perhaps this might be an opportune time for remote controllable device manufacturers, as well as for relevant standards bodies, to begin setting the stage for more protected, perhaps encrypted and authenticated remote control schemes similar to those already being used in garage door openers and higher-end car remote controls. But the need for these precautions is not limited to TVs -- it extends to virtually every remote controlled device including those that reach out and touch the Internet.

Don't give in to electronic terrorism! It would be a shame -- and potentially a huge tragedy -- for a country's infrastructure to be at the mercy of both local and remote control by the disaffected, or by unfriendly governments.

Now is the time to make Internet security job one.



www.futurebrief.com

Don't Blink!

This essay is original and was specifically prepared for publication at Future Brief. A brief biography of Jeff Harrow can be found at our main [Commentary](#) page. Other essays written by Jeff Harrow can be found at his [web site](#). Jeff receives e-mail at jeff@theharrowgroup.com. Other websites are welcome to link to this essay, with proper credit given to Future Brief and Mr. Harrow. This page will remain posted on the Internet indefinitely at this web address to provide a stable page for those linking to it.

To download a PDF version of this essay, [click here](#). Please feel free to share the PDF with others who may be interested. To hear about future **Commentary** essays, take a few seconds to read about [Daily Brief](#), one of the "briefest" Internet updates offered anywhere.

© 2005, Jeffrey Harrow, all rights reserved.