Fred Cohen & Associates - Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Another ridiculous cyber warfare game to scare deciders into action

The advertisement and public relations were highly effective, as the national media reported first that there would be a cyber warfare game, then the leaked results, then the private release by government groups to "insiders", then the public version, and soon (now) the replay. The game - the real game - is the public relations game - sponsored by some powerful and wealthy financial interest groups - dedicated to scaring the public and the politics into action - to send more money through the fear machine - and it's good for the economy!

The scenario as I last heard it

A cell phone virus exploiting interest in the college basketball tournament, gets downloaded into and infests 60 million cell phones, which then shuts down the Internet (or was that a separate scenario - the facts are not yet available), which then takes out the power grid for a week or more, and the lights in the simulation room are still on with simulated video feeds from the news media. What's wrong with this picture? Hmmm....

- The basketball nexus is clearly directed at Obama to create the notion that it's feasible that 60 million cell phone users would be infected by the thing. Nice perception management approach - a bit obvious - but it might well fool the White house.
- Are there 60 million cell phones in the US using the same technology spread across a variety of networks? I just ask because, if not, then that part of the scenario is a bit of a stretch - OK a lot of a stretch. And that's a lot of basketball fans all downloading the same cell phone code with nobody noticing the Trojan. You do know that some people actually run software ahead in time and look at code and test things out and look for changes at a low level? So as the numbers grow, so does the likelihood of detection.
- And by what bizarre notion does anybody actually believe that 60 million cell phones doing anything would shut down the Internet? The actual networks with their towers don't support the bandwidth in simultaneous use by very many phones, but even if they were all broadcasting all the time at maximum bandwidth, they would only do so for a few hours before running out of power. And then? Of course the actual cell infrastructure is largely overloaded lots of the time today, so we are, at times, near peak utilization anyway. But as I said, it is unclear whether the Internet shutdown in the scenario was a cascade effect of the cell phone attack or not.
- So suppose it's a separate attack that stops the Internet, the whole Internet, the most redundant system of all time, with no central control, with distributed everything, that crosses global boundaries. OK - a DNS attack might have a large-scale effect, but that would not stop many of the financial transactions, or most of the power control systems, and the effect takes significant time because DNS is cached... on so on... But wait! I know what could shut down the Internet. If we gave control to the government!!!
- How are we supposed to buy into the notion of the Internet shutting down will stop us

from being able to deliver power? The wind mills, nuclear plants, coal plants, solar panels, and water turbines don't really require Internet to generate power. The wires that deliver the power do not use the Internet protocol to deliver it. While the supporting infrastructure is partly controlled by IP-based systems, an Internet outage is unlikely to have a massive effect on power today.

- And by what wild mind's exaggeration do we believe that these most serious effects will remain for a week? Didn't anybody in the game recognize that we have millions of people who will work to fix it? Don't the people who try to run these games understand that there are real experts who will actually go out into the field and make things work? And don't they get it that the utility workers are not infected by viruses even if their computer is? They will respond - in one way or the other - and things will not be as bad as the crazy claims of such games make them out to be.
- And tell me - how exactly is it that when there is no communication and no power working, that the lights in the simulation room are still on and the video news media is still operating? Gosh - I know how to solve the problem - let's just take the power from the simulation room and run it backwards to feed the rest of the power grid...

Fear not - the scenario will change...

Now I have been here before. And I know the response to my concerns. Here is a sampling...

- You (Fred) miss the point. (No - I don't.) This is really about [fill in the blank] - and the details of the scenario are minutia. (No - it is not - and they are not).
- You (Fred) don't know what actually happened. (That's right - I don't). The actual scenario was [different versions from different folks]. (The actual scenario is what I described - an exercise in inducing fear to generate increased fear responses and get money for the sponsors - and it's not a game - and it's still running).
- The scenario was validated by [somebody that is supposed to make me believe that it's valid]. (And now it has been invalidated by me. In addition to being validated by someone who claims to know more than you or I, it also has to actually make sense.)
- You always do this sort of thing Fred. We're tired of it. (Get used to it. It's called free speech. My Web site is still up and your scenario won't be taking it down.)

So what's the point?

I don't mean to say that we don't have serious challenges to be met in information protection. I mean just the opposite. We have very serious challenges. And the first challenge is getting at the truth through a scientific approach, not promoting or allowing others to promote fear.

Strategic scenario simulations are designed to create and alter perceptions and explore a space. But it is hypocrisy when it is done by those who benefit from the fear they generate. The last time I brought up the hypocrisy behind the fear machine started shortly after 9/11, when folks were trying to promote similar fears to get funding for a war. And look how great that turned out! **Don't get fooled again, again!**

