3-1-2005

Killing the Chickens to Frighten Monkeys

Jeffrey Barlow
Pacific University

Recommended Citation
Killing the Chickens to Frighten Monkeys

Rights
Terms of use for work posted in CommonKnowledge.

This editorial is available at CommonKnowledge: https://commons.pacificu.edu/inter05/14
Killing the Chickens to Frighten Monkeys

Posted on March 1, 2005 by Editor

By Jeffrey Barlow <barlowj@pacificu.edu>

My daughter Clare, now a freshman at Pacific University, recently received a somewhat lower grade than she expected on an assignment in a Political Science class. The assignment had been to model an Op-Ed type of policy discussion. Her grade was lowered, the instructor explained, because while she had outlined the problem very well, she had not suggested a solution. By those standards, this editorial, too, should be marked down. I can outline the problem easily, but the suggested solutions are at best partial ones.

The problem is that the Berglund server, appropriately named “BCIS,” was hacked about a month ago, shortly after we posted our February issue. We heard from a number of readers (and some authors) in this period that we were not available on the Internet. We were unable to make full explanations to all queries, so we hope those same kindly souls are reading this editorial.

Our systems operator had been aware for some time that someone has attempting to enter our system, usually probing it on weekends. The usual result was that the system crashed, requiring a tedious re-start late Sunday night each week. As the hacker was unsuccessful we ignored these warnings, feeling that they showed at best that we were adequately protected. And as well, we had a regular strategy of backing up our disks each week. It seemed to us that we were O.K.

Then one weekend we did not crash, but rather received complaints from other sites on the Internet that our machine was mounting denial-of-service attacks on their machines. [1] Our machine was flooding other machines with spurious messages intended to overwhelm them, taking them off-line. By 10:00 A.M on Monday we had received two of these, both of which had first gone to our Systems Operator at Pacific University.
We also received a very thoughtful letter from an entrepreneur in central Europe, in effect inviting us to explore purchasing additional software or security programs from him so as to prevent such outrages. He had, it was explained, noticed the penetration because his software relentlessly scanned the World Wide Web looking for just such enslaved machines mounting Denial-of-Service attacks because these had a typical pattern which he could identify.

These Denial-of-Service attacks are, generally speaking, little more than hacker’s exploits. They are not difficult to mount, nor is there any financial advantage in doing so, unless they are connected to some sort of protection racket in which the criminal offers to somehow prevent them, as by showing the firm impacted how to prevent them.

In theory at least, this is not only a criminal matter, but a potentially serious one. In our case, for example, some federal work-study monies pay for our student work to maintain the server, and thus the attack on us triggers laws enabling us to call in the F.B.I. In reality, of course, these attacks are so common that the F.B.I. would be more inclined to lecture us on our security failures than to undertake an investigation.

And our failures were many. We had not regularly updated some of the programs through which the criminal apparently entered. It was just not part of our routine to check for security patches on minor operations such as a BBS created to serve academic classes and our Trans-Pacific Interactive Classroom project, discussed elsewhere in this issue. (See Yang De-sheng’s article at: http://bcis.pacificu.edu/journal/2005/02/desheng.php). It was apparently through an old version of the BBS program that the attacker entered, a weakness that he or she turned up after weeks of probing.

In addition, we found that our file back-ups were, in several cases, flawed. The backup program was writing to protected disks as we assumed, but it was not always writing retrievable information. We lost some non-essential files and had to go back further in time for our restorations than we had planned. We thought we were backing up nightly. But in some cases the usable backups were weeks old. Obviously this could have been far worse. We had some very anxious hours in which we thought it possible that we had lost years of work by many authors.

And we did lose many hours of student time. The total cost to us was in the realm of about one hundred hours of student support time at ten dollars an hour. It is easy to imagine a cost of many tens of thousands of dollars at larger operations than ours, or at commercial firms.

So what is the solution? The first impulse, of course, is to somehow hunt down the criminal and kneecap them in the IRA style. Not only is this unethical behavior on our part, it is also impractical. The F.B.I. can hunt down cyber criminals because they have the computing power and the legal authority to work through a maze of false electronic identities, as well as more sophisticated means of trapping them. We do not.
The Chinese historically practiced Draconian enforcement of laws and mores by “Killing the Chicken to Frighten the Monkeys.” That is, picking out what may have been a lesser offender and so punishing them that more major criminals of the same type would be warned. That seems to me to be about where our legal system is at present, and our ability to protect the Internet and our systems by preventing crimes. We can pick out occasional teen-agers and make public examples of them and their families for illegal hacking, file sharing, etc.

But given the very small percentage of such successful prosecutions, not to speak of their dubious morality, this path seems unlikely to lead to a golden age in which we can again neglect our security patches. Our anger is such at the costs of our own little incident that we would probably have been happy to have had blood and feathers up to the ceilings of our labs. But ultimately, our security is now up to us.

What lessons have we derived for our own operations?

- We need to cleanly identify all programs running on our machines and continually scan for updates and patches. This will be time-consuming and may be expensive as it means a continuous process of updating applications that are serving us well because they have been identified as accessible within the hacker community.

- We need to be more conscious of the quality of our updates, even to the point of having periodic update drills in which we attempt to restore programs and content on stand-by machines so as to be sure that we can restore service in a short time with minimum efforts. This too, will be expensive and it will be difficult to maintain as other programs and problems prove pressing. But the alternatives are not good ones.

We suggest that if you have not recently protected your own systems, you do so.

Jeffrey Barlow
Director, Berglund Center for Internet Studies
Pacific University


This entry was posted in Uncategorized by Editor. Bookmark the permalink [http://bcis.pacificu.edu/interface/?p=3085].

16 THOUGHTS ON “KILLING THE CHICKENS TO FRIGHTEN MONKEYS”
twin hcg weight lifting florence hotel reservations cardinal parallel emulators
ryan scheckler seadoo on
on February 3, 2014 at 11:08 PM said:

Wow, this piece of writing is good, my younger sister is analyzing such things, so I am going to inform her.

post surgery
on February 3, 2014 at 11:27 PM said:

I’m really enjoying the design and layout of your website.

It’s a very easy on the eyes which makes it much more enjoyable for me to come here and visit more often. Did you hire out a developer to create your theme?
Superb work!

Della
on February 4, 2014 at 12:09 AM said:

If you would like to take a good deal from this post then you have to apply these techniques to your won webpage.

nigeria
on February 4, 2014 at 10:17 AM said:

One extra process in favor of advertising your website is posting comments on various directories within your blog link.

nigeria entertainment news
These days the internet technologies offer us having a very certain possibility to choose what exactly a single requires.

---

**nigeria entertainment news**

on February 4, 2014 at 10:37 AM said:

It is my belief that mesothelioma is most lethal cancer. It is got unusual features. The a lot more I look at it the greater I am assured it doesn’t conduct itself as a actual solid tissues cancer. During the event mesothelioma is really a rogue virus-like infection, then there is the prospects for developing a vaccine plus offering vaccination for asbestos uncovered those who are vulnerable to high risk connected with developing lengthy term asbestos associated malignancies. Thanks for discussing your ideas about this significant ailment.

---

**Cole**

on February 4, 2014 at 1:16 PM said:

Wow, this piece of writing is nice, my sister is analyzing these kinds of things, therefore I am going to convey her.

---

**mobile video**

on February 4, 2014 at 3:01 PM said:

I like looking through an article that will make men and women think. Also, thanks for allowing me to comment!

---

**business directory listings**

on February 4, 2014 at 6:26 PM said:
Your mode of describing the whole thing in this post is in fact good, all be able to simply understand it. Thanks a lot.

---

**Kristina**  
**on February 4, 2014 at 6:44 PM** said:

Hi my loved one! I want to say that this article is awesome, great written and include almost all vital infos. I’d like to peer extra posts like this.

---

**network marketing mentor**  
**on February 4, 2014 at 8:27 PM** said:

Every weekend i used to pay a quick visit this web site, as i wish for enjoyment, for the reason that this this site conations really good funny stuff too.

---

**earn money online za**  
**on February 4, 2014 at 11:38 PM** said:

Wow, that’s what I was exploring for, what a information! existing here at this website, thanks admin of this web site.

---

**make money online gta 5 ps3**  
**on February 5, 2014 at 4:28 AM** said:

Superb blog! Do you have any recommendations for aspiring writers? I’m planning to start my own blog soon but I’m a little lost on everything. Would you propose starting with a free platform like WordPress or go for a paid option? There are so many choices out there that I’m
totally overwhelmed .. Any ideas? Bless you!

---

**Scott**  
on **February 5, 2014 at 12:23 PM** said:

Hi, everything is going sound here and ofcourse every one  
is sharing information, that’s really good, keep up writing.

---

**Zachery**  
on **February 6, 2014 at 12:37 AM** said:

Hi! I just wanted to ask if you ever have any issues with hackers?  
My last blog (wordpress) was hacked and I ended up losing several weeks of hard work  
due to no data backup.  
Do you have any solutions to prevent hackers?

---

**Shirleen**  
on **February 6, 2014 at 4:32 AM** said:

You made some good points there. I looked on the net to learn more  
about the issue and found most individuals will go along with  
your views on this site.