

The Heads and Tails of Information

By Ronald Baklarz Jr., CISSP

“Information has an inherent duality – a Yin and a Yang, a dark side and a light side, fullness and emptiness, solid and liquid. It resides at the crossroads between data and knowledge.”

Sensei Sun

The Art of Information Warfare: Insight Into the Knowledge Warrior Philosophy

The other day I happened to be scavenging through my e-mail's overfilled inbox where I happened across an old message containing a link to the wonderful ZDNet web site. Curiosity as to why I saved this link got the best of me and with the click of the mouse; I was confronted with an article discussing the *10 Most Wired Colleges for 1998*. Instantly, the sixth sense of the *Knowledge Warrior* activated and I immediately envisioned the potentially disconcerting aspect of this seemingly innocent and positive article. Reams of paper began spewing from my mind's imaginary printer. Upon closer review, the flowing paper revealed millions of cryptic lines of log data from our corporate firewall. Even closer examination of the log data showed millions of lines of data each depicting nefarious attempts to cause heinous harm to the corporate IT infrastructure. Without physical movement on my part, my mind instantly evoked a counter-barrage of *pings*. *Trace routes*, and *whois* queries against the offending IP addresses as identified by the firewall's log data. As you may have guessed, each of the responses to those queries came back like typed pages from Jack Nicholson's manic novel in *The Shining*. While Jack's novel consisted of thousands of pages with the same sentence “*all work and no play make Jack a dull boy*” repeated on each line, my novella of firewall log data depicting attacks hauntingly echoed: “.edu, .edu. edu...”

I awoke from the nightmarish daydream in a cold sweat and reflected on its meaning. I am in no way advocating that our universities and colleges should not be connected to the Internet, quite the contrary. There is much more in the way of good to be gained from Internet connectivity than bad. But as a security professional, the information provided in the *Most Wired* article, scared the hell out of me as colleges and universities have historically been hotbeds of hacker activity. The article not only discussed the college rankings, but the various metrics used to determine just which college should earn the *Most Wired* title. Seemingly innocent data points such as the college's use of their intranet web sites for disseminating student information gave way to potentially dangerous numbers such as network port-to-bed ratios, percentages of students who owned PCs, and the number of publicly available computers (PAC's). The latter three data elements caused the hair on my skull to stand on end (which is probably easy for them to do given the sparse foliage).

Let us consider the data element PAC or the number of computers on campus that are available to the public. Now as Mr. Rogers would say, “Can you spell a-n-o-n-y-m-i-t-y ?” I can only imagine the potential for these types of computers to be used as attack platforms for which there is no trace to the original perpetrator. The ZDNet analysis also included anecdotal factoids regarding each of the colleges. The factoid connected to CMU – Carnegie Mellon University in Pittsburgh, PA was particularly interesting. It read, “CMU has more networked computers on campus than the entire university population.” Therefore, I have to question the PAC figure of 364 at CMU. While 364 may be the number of computers that are *legitimately* available to the public, I'll wager that there is a significantly higher number that *can* be accessed by the public. Actually, my first attempt at ethical hacking occurred in the mid-1980s when I worked for Westinghouse Electric Corp. and the Naval Nuclear Program. I was taking a graduate class at the University of Pittsburgh that was taught by a moonlighting professor from CMU. With the professor's knowledge, I was able to gain access to the Sun workstation on his desk at CMU through a TCP/IP stack on an UNCLASSIFIED (thank god!) mainframe located in the middle of the great state of Pennsylvania via a terminal located in a suburb of Pittsburgh. While I cannot vouch for the security configurations at each of the *Most Wired* schools, we must be vigilant for potential abuses. Other scholastic factoids that were equally disturbing to my *Knowledge Warrior* persona were:

- *Illinois is home to the prestigious National Center for Supercomputing Applications.*
- *Students at CAL Tech can sign up for high-bandwidth cable modem access to the Net.*
- *Advanced Net users at Worcester Polytechnic Institute like to maintain their own hubs in the residence halls*

Below is the list of the *Top 10 Most Wired Colleges* identified per the ZDNet article. I have also identified the approximate IP ranges of each school just in case they show up on your firewall logs -- in reality or in your nightmares.

College Name	1998 Rank	PAC's*	% of students w/computers	Approximate IP Address Range
Dartmouth College	1	122	100	129.170.0.0
New Jersey Inst. Tech.	2	4015	100	128.235.0.0
MIT	3	900	85	18.0.0.0-18.255.255.255
Rensselaer Polytechnic	4	618	70	128.113.0.0
Univ. Of Illinois Urb-Chp.	5	3000	40	128.174.0.0
CMU	6	364	76	128.2.0.0
Cal. Inst. Of Tech.	7	600	50	131.215.0.0
Indiana Univ., Bloom.	8	N/A	50	129.79.0.0
Univ. of Oregon	9	N/A	70	128.233.0.0
Worcester Polytech.	10	1000	75	130.215.0.0

Again, I am in no way blaming anyone for anything. I am merely pointing out the *dark side* of this information. If colleges are not taking responsible actions to secure their networks and Internet connection points, this area may prove to be increasingly problematic in conjunction with increasing numbers of technically savvy students. Colleges and universities have typically been havens for hacker's and launch pads for attacks and I see things getting only worse. Recent postings on the Intrusion Detection newsgroup have supported this position. One June 1999 posting stated: *"I have 2 .net, 1 .com, and 1 .edu domain that can be transferred. What is interesting is that every single unauthorized zone transfer has been for the edu domain. This leads me to believe that .edu sites are popular starting points for many of today's script kiddies. Have others seen this pattern?"* (A zone transfer is a function of Domain Name Services (DNS) where one can derive listings of a site's internal IP (host) addresses, or *potential targets*).

In the future, I hope to update this article in conjunction with ZDNet's annual survey update. I am holding my breath in anticipation of the *Top 10 Wired High Schools*.