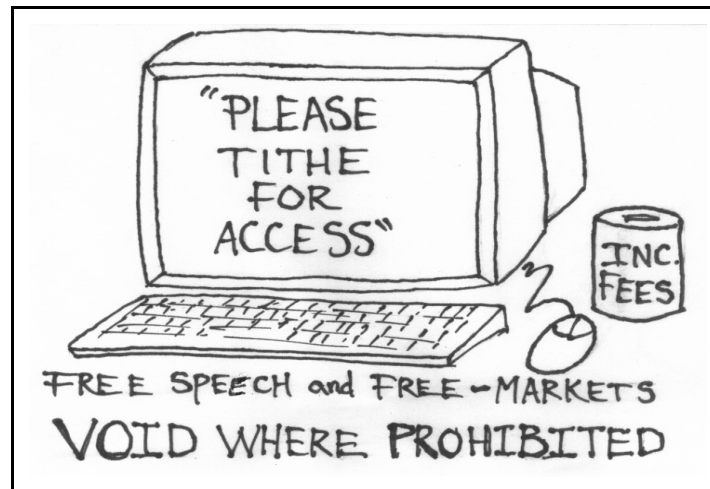


# The Cepia Club Paper Series #4

Informational Series of The Cepia Club

February 15, 2007

## Computerized Nation: Issues on Security and Freedom



### A Brief And Incomplete History Of Malicious Code; And A Short Look At The Future

By Charles M. Barnard

Unfortunately, the time to start working on security against malicious code was 35 years ago--when such code was first predicted. (See *Shock Wave Rider* by John Brunner.)

Too little thought to security issues is given by Operating Systems (Os) providers--so

little, that it appears that they spend little or no time testing for vulnerabilities (notice Vista already has public vulnerabilities....)

Code can and will be written to steal or abuse \*anything\* -- and it becomes easier every month (Moore's law again....)

For example, the first internet viruses in the early 90's (and the disk based viruses before then,) were primarily created by very bright people as the knowledge needed to write a successful piece of code was considerable.

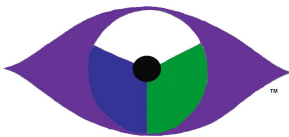
Also, these viruses were incredibly 'dumb' nearly all of them merely (and often immediately) destroyed data, making public their existence very rapidly. Many of these were written with the main intent of showing system vulnerabilities. OS manufacturers were reluctant to admit bug much less security issues.

At about that time ATM's appeared, and it was several years before any of them were even insured against such lose, much less using even the simplest encryption of data lines--it took a number of large losses before the banking

industry would admit that there might be an issue

Shortly thereafter, virus generators became available, and the required intelligence to create a virus plummeted, and the number of virus originators skyrocketed.

Still, at the time, and for a few years more the common malicious code wasn't designed to steal effectively, but to destroy and reproduce.



**The Cepia Club**  
**P.O. Box 60**  
**Osceola, WI 54020-0060**  
 715-268-2963

Visit  
[WWW.CEPIACLUB.COM](http://WWW.CEPIACLUB.COM)

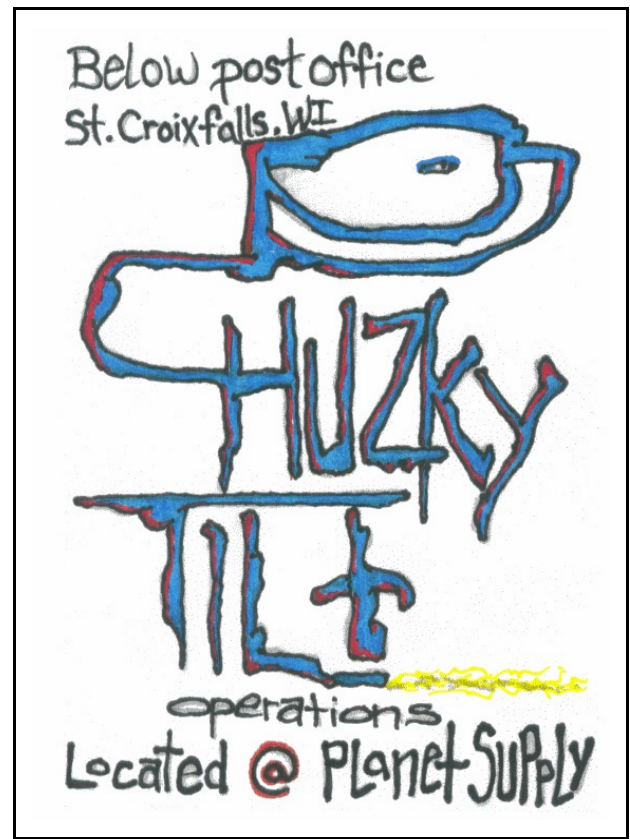
*Publications, Broadcasting,*  
*CepiaNet,*  
*and Public and Media Relations*  
**"Connecting people. . ."**

Now we have a growing market for malicious code designed to actually steal physical goods and money. This is much more difficult than generating annoying code; this requires the level of effort and knowledge that the original virus writers needed...thus a

sellers market. One of the main advantages of selling the code is that writing and selling such code is perfectly legal—and there is no good way to put in place a mechanism to enforce any laws written to change that fact.

Money is of course, easier than physical objects, since the vast majority of money is now electronic, and has no physical existence unless desired. Of course, stealing electronic money and converting it to physical currency permits a "break" in the audit trail for the money—once currency is issued it becomes very difficult to trace. This is not a new of course; illegal transactions are usually in cash for exactly this reason.

Physical goods have been stolen with information systems since at least the late 1960's—the freight moves on a paper trail—which is now data. Additionally, the shipping couriers (FedEx, UPS, etc.) are in a fight to provide the fastest most convenient delivery system for their customers: You can get



packages delivered to nearly and time and place. Again, once the theft is converted to a physical object, the trail disappears.

Nearly all of the things being done maliciously with code are variations of tried and true ancient methods merely updated to work remotely and electronically. The actual problem is created, in part, because electronic theft can be carried off and even covered up in well under a minute; many times in a matter of milliseconds.

By the time a theft is discovered, hours to weeks may occur, leaving a very cold trail.

I haven't seen any code designed to the specifications I wrote in the 1980's:

- 1) Stay hidden. If necessary delete all references to your existence and yourself to preserve secrecy.
- 2) Reproduce.
- 3) Steal anything which appears of value.
- 4) Update yourself based upon what you learn while skulking.
- 5) Transmit what you learn to your owner and other copies to yourself. (Some sort of drop box method would work. There are lots of places to 'temporarily' store stuff. The most unusual, which I haven't yet seen done, is to keep the information cycling through the network.)

One method of dealing with enforcement improvements is to blanket the systems with thefts in which the swag goes to an innocent third party—generating a huge database of suspects.

Malicious code will never go completely away: No software or auditing system will ever be perfect. The best defense would be to develop AI to the point that an AI could do vulnerability testing on a batch of code, and develop defenses against such vulnerabilities.

We desperately need adaptive code identification—a 'stealth' worm could transfer billions of dollars before it was even recognized in the wild.

We also need a method of encryption and certain identification for interactions between computers. All traffic should be both encrypted and identified properly as to the sender.

It would be best if such methods could be designed as hardware, (though, of course, firmware can be hacked, too, it is more difficult to change it remotely.)

I suspect that computers and programs will always be somewhat 'ill' as are most animals including humans. And as with animals, the illness can be in the hardware/wetware or the software/behavior. And we only started learning about behavior illnesses in the past century and have yet to develop really good methods of diagnosis or treatment; we only recently discovered that many "behavior" illnesses are actually wetware based.

**Now available only  
from  
The Cepia Club!**

***The Mad  
Tales***  
by Pi Kielty

A collection of short stories,  
poem, and essay by The  
Cepia Club's own persona  
mira.

**ORDER TODAY!! Send  
address &  
check for: \$10.00  
(includes shipping and  
taxes)**

**To: The Cepia Club  
P.O. Box 60  
Osceola, WI 54020**

**Net Neutrality &  
Liberty**

By Charles M. Barnard

Historically, there have been two main ways of looking at data traffic: the telephone model, and the broadcast/cable model. Under the telephone model, the carriers (people actually moving the signal) cannot treat any signal differently than any other signal. All conversations are equal.

Under the broadcast/cable model, transmissions are

*expressions* (i.e. public works) and the carrier has discretion about how they handle the signal—including the right to censor.

The argument is about whether Internet data streams are subject to telephone *common carrier* rules or broadcast/cable *discretionary* rules. Because of the blurring of the differences between the two systems on a

cost several hundred times what a voice connection cost.

Obviously, if the carrier(s) can determine what content they transmit, your liberty to transmit the data you wish is severely limited, at least in theory. But in liberty that does not harm others, can there ever be compromises and still call it liberty?

**About the Author:**

Charles M. Barnard is the owner and operator of [www.wizodd.com](http://www.wizodd.com), a computer and technical support business.

The Cepia Club Paper Series #4  
A publication of:  
The Cepia Club  
PO Box 60  
Osceola, WI  
54020  
[www.cepiaclub.com](http://www.cepiaclub.com)

Copyright © 2007 The Cepia Club  
All Rights Reserved

The Cepia Club Paper Series is a collection of essays dealing with political, economic, cultural, and social issues confronting communities. The views contained herein belong solely to the author(s).

Advertisers with The Cepia Club neither endorse or oppose any Club positions, statements, ideas, or programs. They are independent businesses contracting for advertising.



Join the CepiaNet!

Sign up for the Yahoo! Group at:

[WWW.CEPIACLUB.COM](http://WWW.CEPIACLUB.COM)

hardware and business level, it is not certain how such signals should be handled legally.

Service providers want to be able to use discretion, not so much to filter, as to permit them to provide differing levels of service based on content and payment. This effectually would permit carriers to block content that they wished, preventing 'free speech' over the Net.

This is similar to the situation in the early days of telephone modem use, when a modem connection in, say Germany,



Box? What box?  
Unusual Problems?  
Unusually apt  
solutions.

[www.wizodd.com](http://www.wizodd.com)

Computer and technical  
support services in  
Minnesota and Wisconsin.

[www.cepiaclub.com](http://www.cepiaclub.com)

Web TV, Radio,  
Publications and More.