Gone Phishin' for Worms . . .
. . . Took Users as Bait

Eric Pancer

epancer@security.depaul.edu

Computer Security Response Team

DePaul University

http://security.depaul.edu

This Talk is Not About Threats

Threat, n.

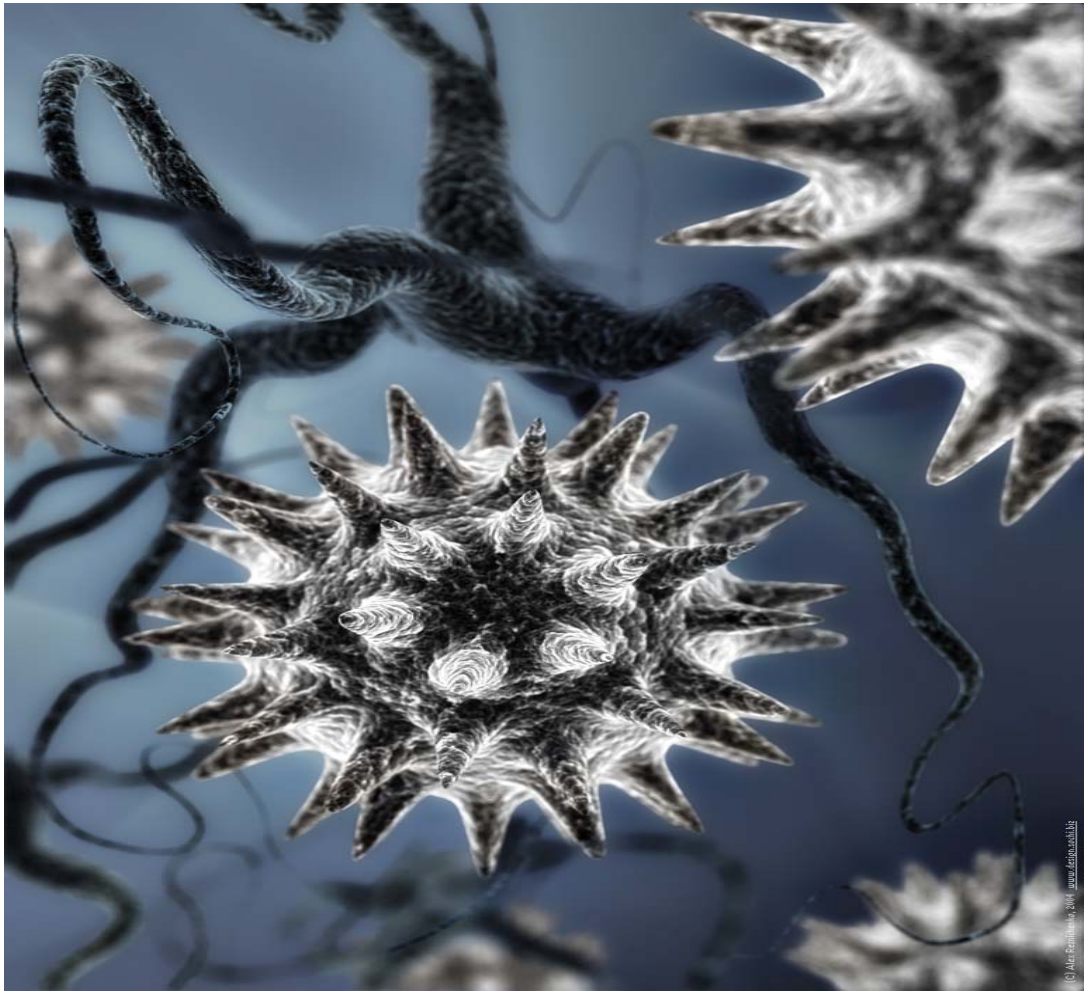
- The expression of an intention to inflict evil or injury on another; the declaration of an evil, loss, or pain to come; menace; threatening; denunciation.

Reality

Reality, n.

- 1. The state or quality of being real; actual being or existence of anything, in distinction from mere appearance; fact.
- 2. That which is real; an actual existence; that which is not imagination, fiction, or pretense; that which has objective existence, and is not merely an idea.

Viruses



The Worm

Spam — For Sale: Smiling Faces

Indecipherable, Junk

Date: Thu, 11 Nov 2004 02:58:04 -0200
To: joe@example.org
Subject: Order Confirmation # 5529 - 707

Dear Fdemissi, If your message below does not load, please Click here to view your important notice!

Thu, 11 Nov 2004 00:56:04 -0400
356*285-4442
EKFTYHGOAPGWA
archwag anisotonic berouged attorneyship Acacian Arthurian begrett authorizable anhydric banaba articulability aeroboat banisher apophysis

PayPal Scam

From: PayPal Support Center <services@paypal.com>
To: Joe User
Subject: Verify and Update your PayPal information

It has come to our attention that your PayPal account information needs to be updated. If you could please take 5-10 minutes out of your online experience and update your personal records you will not run into any future problems with the online service. However, failure to update your records will result in account suspension. To update your PayPal records click on the following link.

<http://www.paypal.com/cgi-bin/webscr?cmd=_login-run>

HTML Trickery

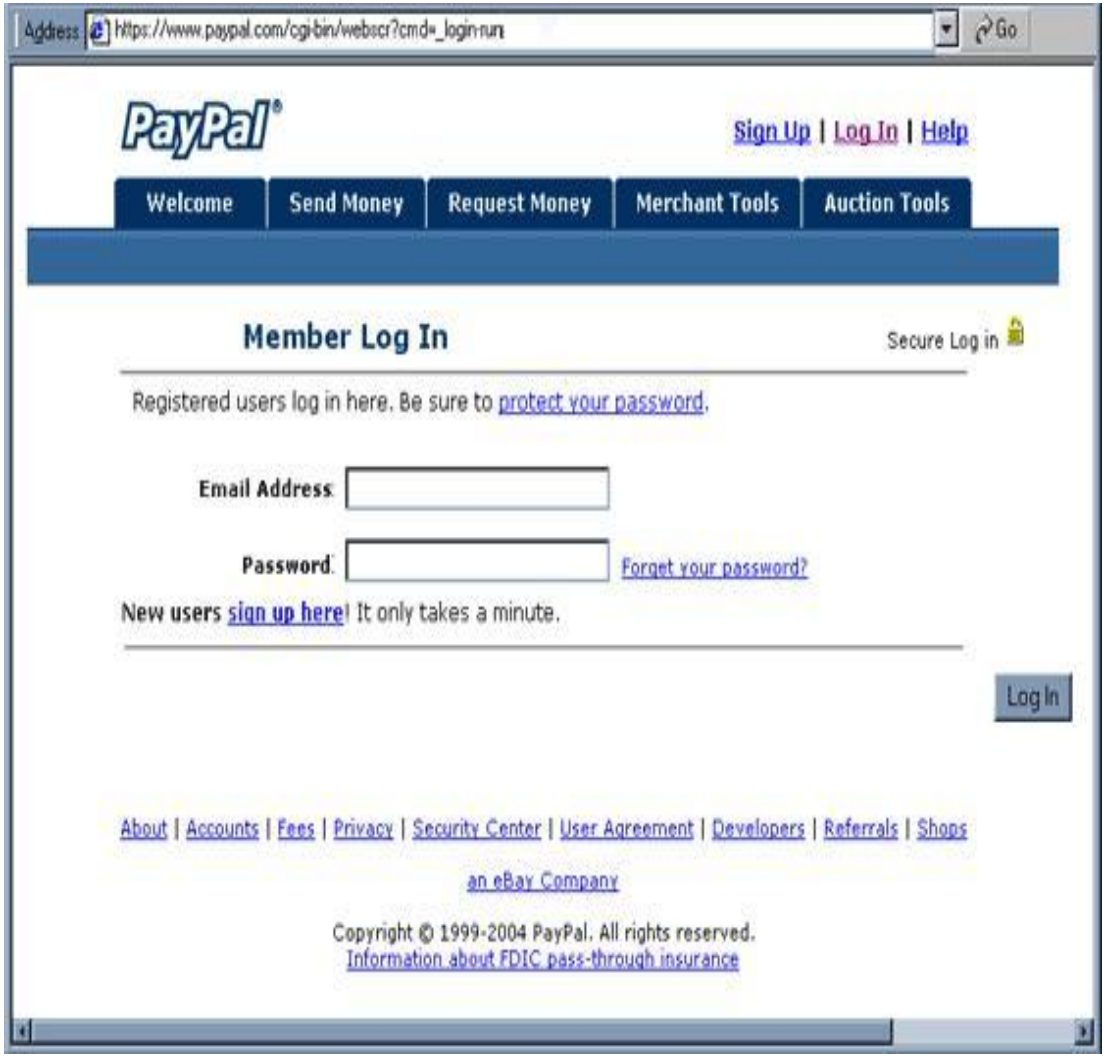
In the previous slide, this link was visible to the user and would be the only link visible to the naked eye in an email.

<http://www.paypal.com/cgi-bin/webscr?cmd=_login-run>

However, this is the embedded HTML code.

```
<A href="http://PayPal.Routed-Team.Org/login.html" target=_self>
 <FONT face=Verdana size=2>
 http://www.paypal.com/cgi-bin/webscr?cmd=_login-run
 </FONT>
</A>
```

Another Play on Reality



Phishing

Phishing takes advantage of the following insecurities:

- Nearly any communication protocol
  - World Wide Web
  - Email
  - Instant Messenger
- Mis/Un-informed User.
- Vulnerable application or operating system.

Come and Get It!

Instant messengers can be an interesting source of malware propagation.

(05:13) sassygirl18: my new pic is online from our party...i was like soooo drunk :-) and could barely stand up! lol http://www.angelfire.com/ar3/sunz/bestfriends.scr

Question: What percentage of 18-24 year old aspiring male students *wouldn't* click on that link?

Blended Threats

Stand alone worms, viruses or spam are so old fashioned! These days the blended, or multi-vector, threat is more common.

- Allows malware authors to bypass firewalls, IDS's, etc.
- Allows malware authors to get a better bang for their buck.
- Can include existing malware as a payload.

W32/Nachi.worm

During August of 2003, the W32/Nachi.worm appeared as the first *major* blended threat.

- It tried to patch W32/Blaster infections exploited MS-RPC.
- It tried to exploit WEBDAV servers vulnerable to attack.
- It was responsible for more ICMP “ping” type packets than many network operators could imagine.

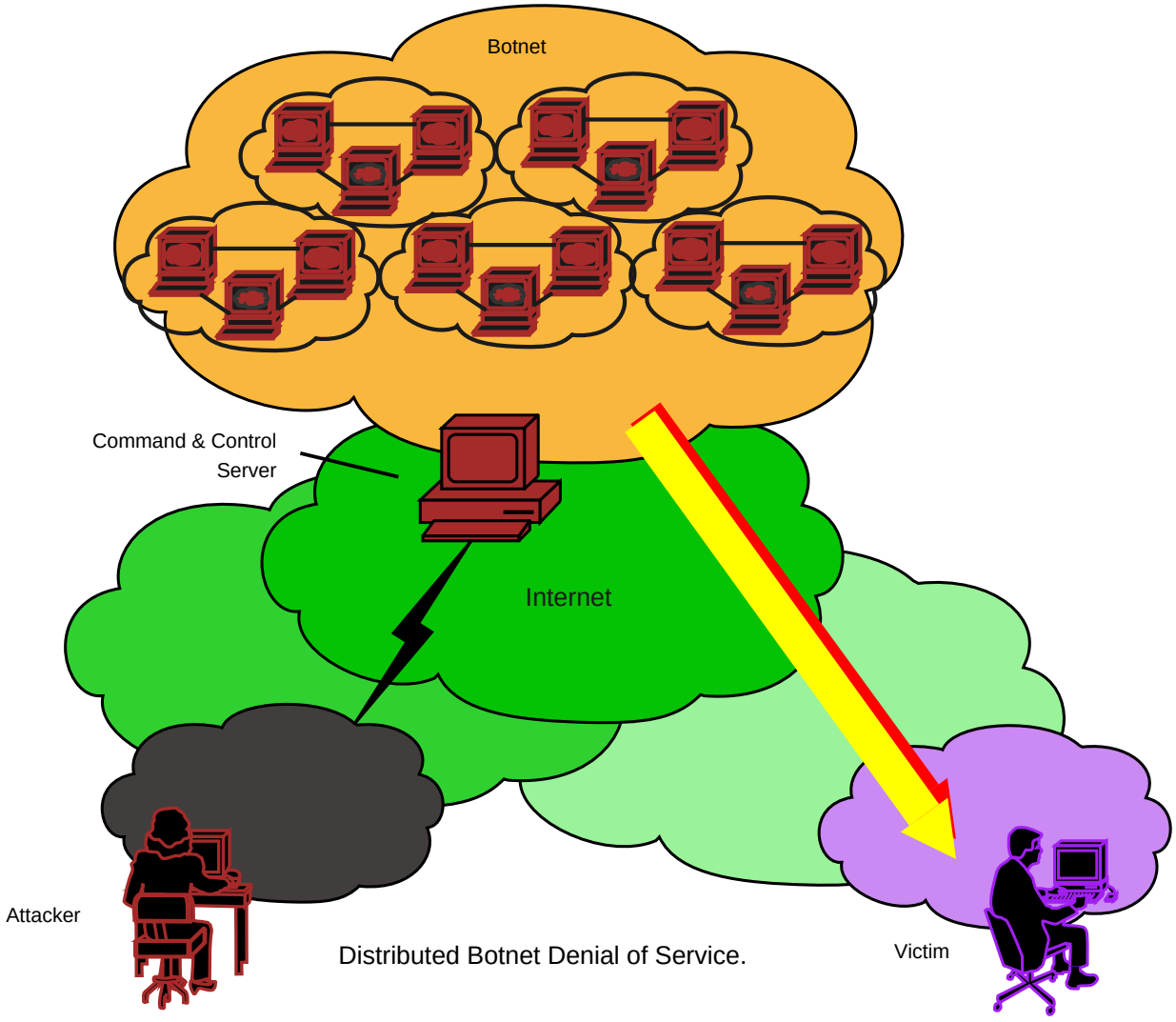
Bots

More prevalent now are “bots”

- Agobot
- SD-bot
- gaobot

Why?

Botnet — A Sample Use



Distributed Botnet Denial of Service.

Who's doing this stuff?

Partners in Crime

Motive

What is the motive for continued hacking, malware writing, etc?

- Easy work-at-home ability!
- It's fun to be a hacker. Tell your friends!
- Law enforcement can't keep up.
- It pays.

You Too Can Be Rich!

Thats All Folks

Thanks for your time.

Questions or comments are welcome!

Email me: <epancer@security.depaul.edu>