



Securing Your Web World



MONEY CHANGES EVERYTHING

New approaches to categorizing economically-motivated digital threats

Anthony Arrott, PhD, David Perry

Trend Micro, Inc.

Virus Bulletin conference, Vienna, Austria, 2007

In the beginning...



- 19 And out of the ground the LORD God formed every beast of the field, and every fowl of the air; and brought them unto Adam to see what he would call them: and whatsoever Adam called every living creature, that was the name thereof.
- 20 And Adam gave names to all cattle, and to the fowl of the air, and to every beast of the field;

That being said...

- This is NOT about virus naming conventions!
- The virus is no longer the main concern
- The individual malware is merely a component in today's attack, used in quantity with a great number of people and servers and complexity
- Maybe we need to focus our defining efforts towards the need of another group of people

THE END USERS!



Confronted with a world of information

Securing Your Web World



PATTERNS alone do not convey MEANING



With so many things to identify



We look to identify PATTERNS



We simplify our approach



We might miss the point



So there is language

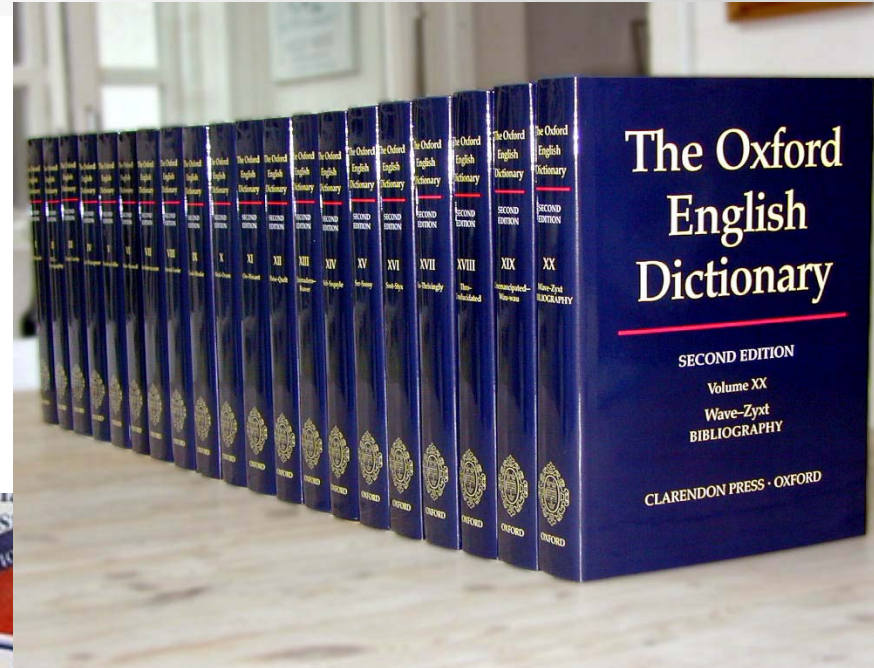
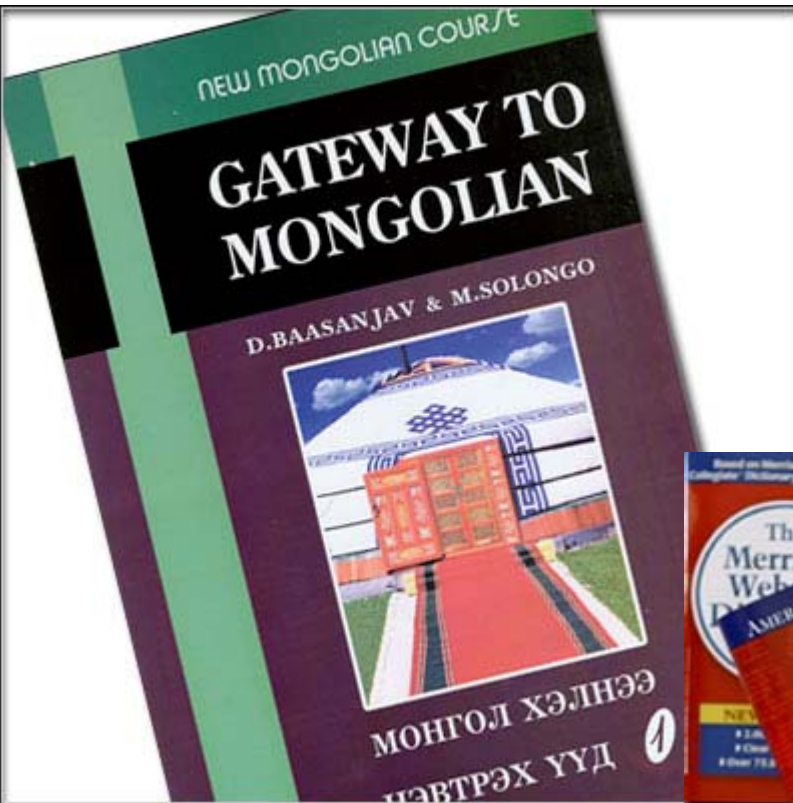


Language also has problems...

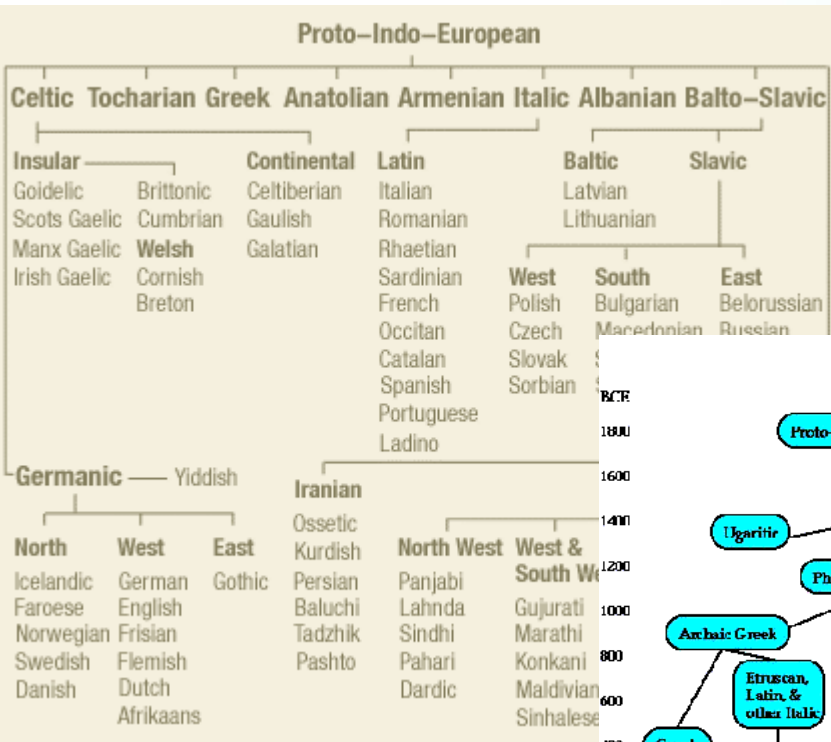
- ***Confusion of map and territory***
- ***Special meaning***
- ***Connotation***
- ***Conflation***



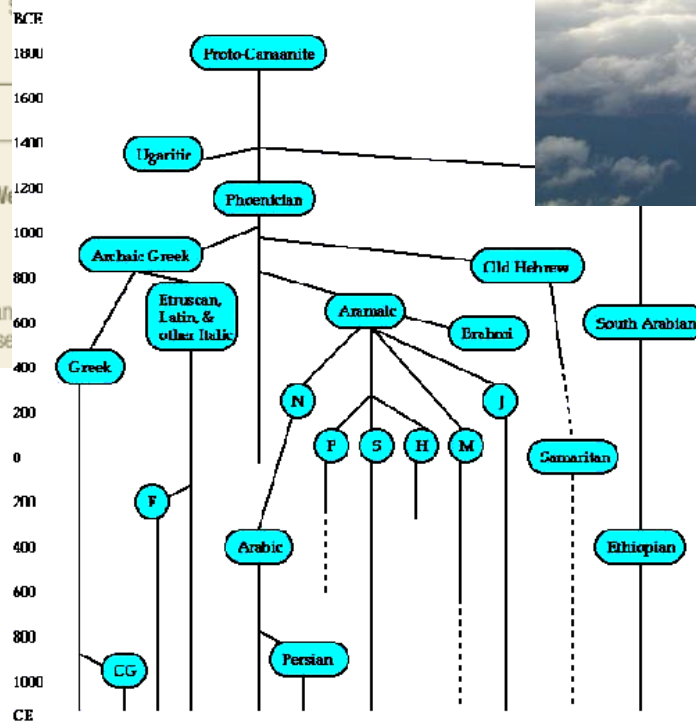
DEFINITIONS



TAXONOMY



Major Alphabets



Greek & Italic Legends

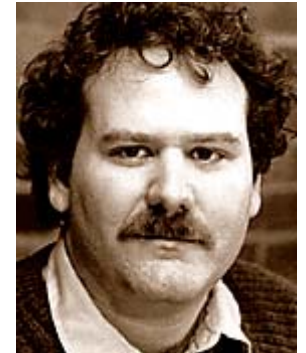
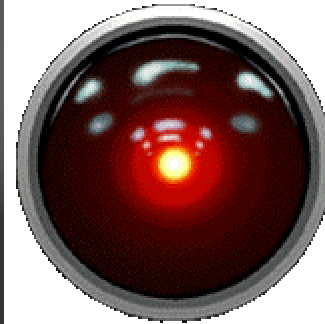
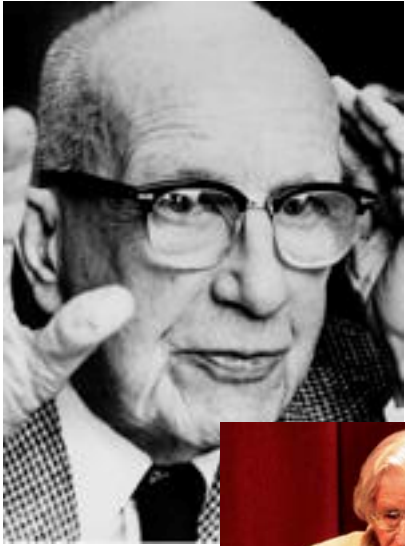
CG Cyrillic & Glagolitic
 F Fullark

Aramaic Legends

N Nabataean S Syriac M Mandaic
 P Palmyrene H Hebrew J Jewish

EXPERTS

Securing Your Web World





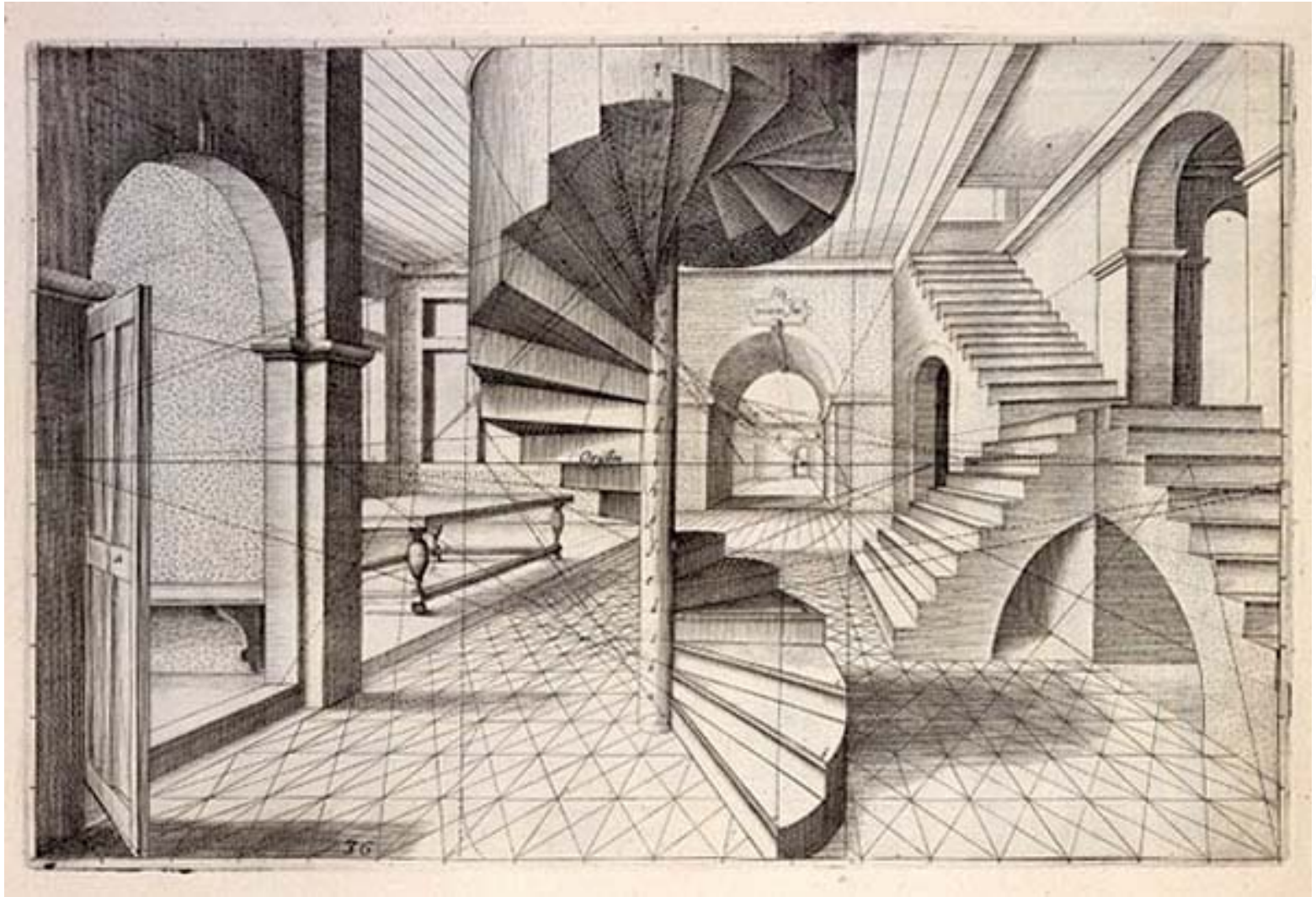
Securing Your Web World



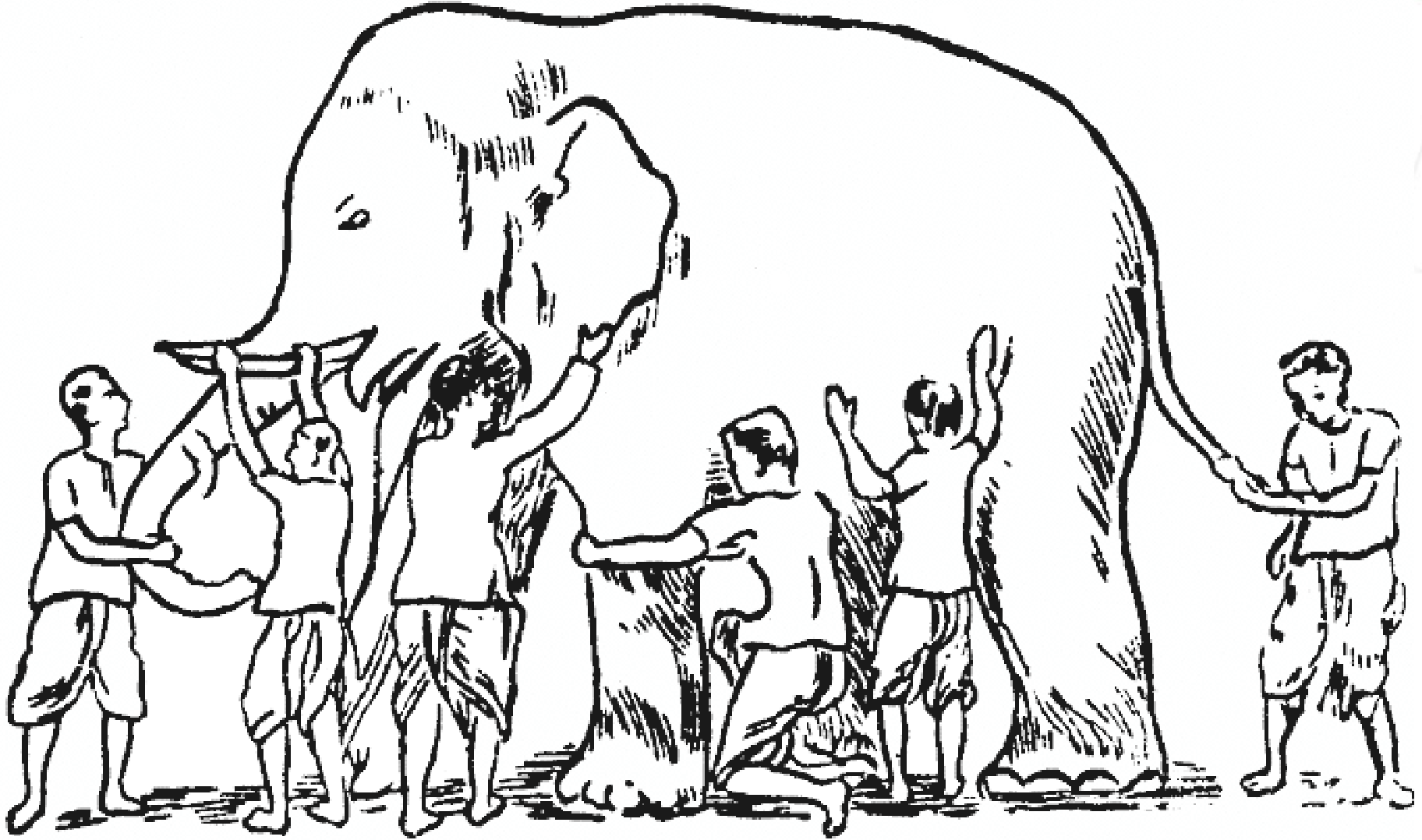
PERSPECTIVE

Patterns and language and perspective=taxonomy

Perspective, in the ideal and in the real world



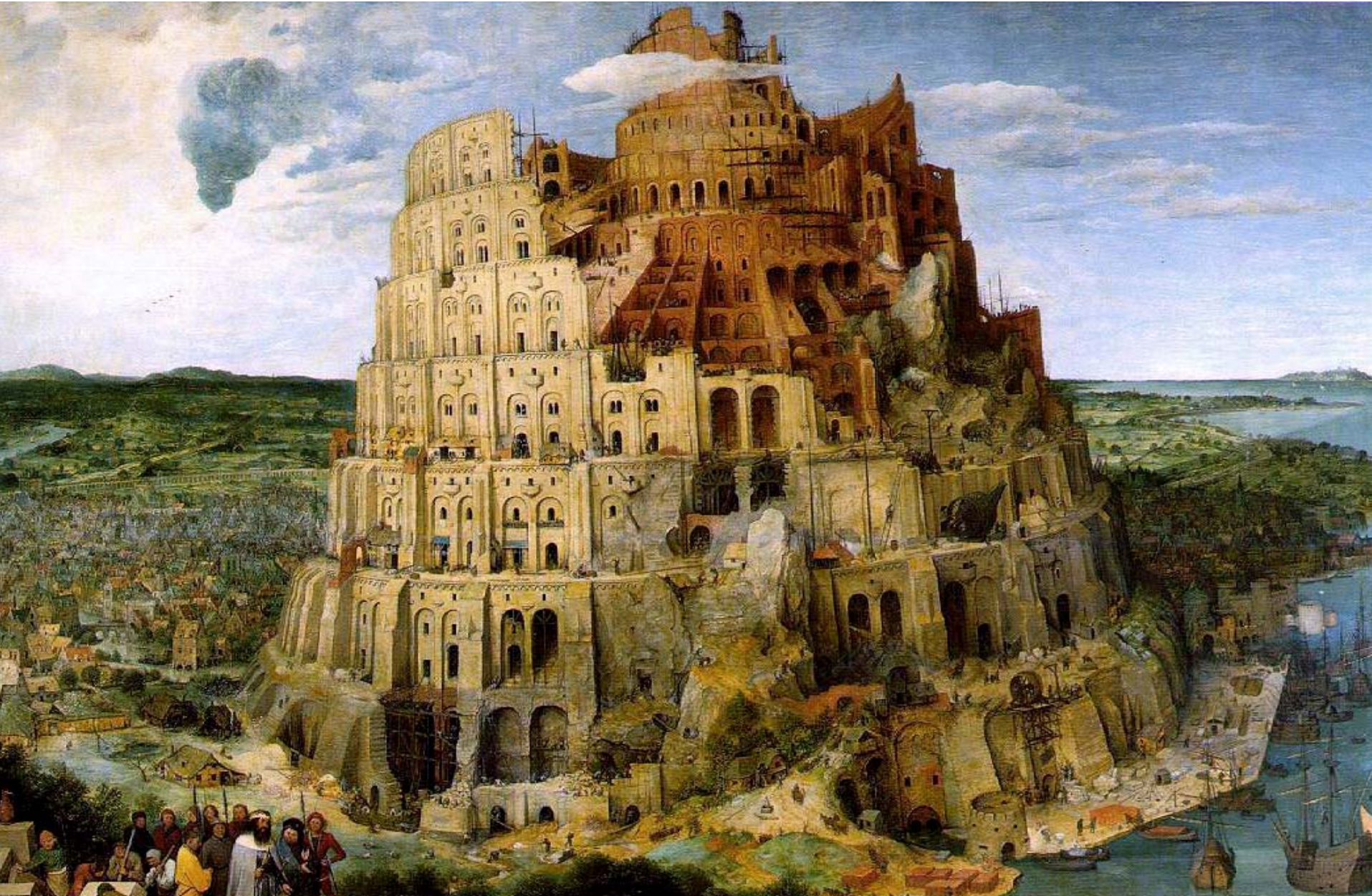
Perspective, in a different metaphor



The virus expert vs the end user

- The virus expert; This particular piece of *malware* is a password stealing trojan, delivered by a downloader connected via a multiple web redirect using iframe and (ad infinitum)
- End user hears: *blah blah blah blah blah*
- End user says: *What does this mean? What is the purpose of this malware?*
- The virus expert hears: *I am a dummy, ignore me.*

This is an impasse of communications



A red horizontal banner with rounded ends. On the left side, there are several white technical icons: a network diagram with nodes and lines, a circular icon with a lightning bolt, and a circular icon with a shield and a lightning bolt. The text 'Securing Your Web World' is centered in white.

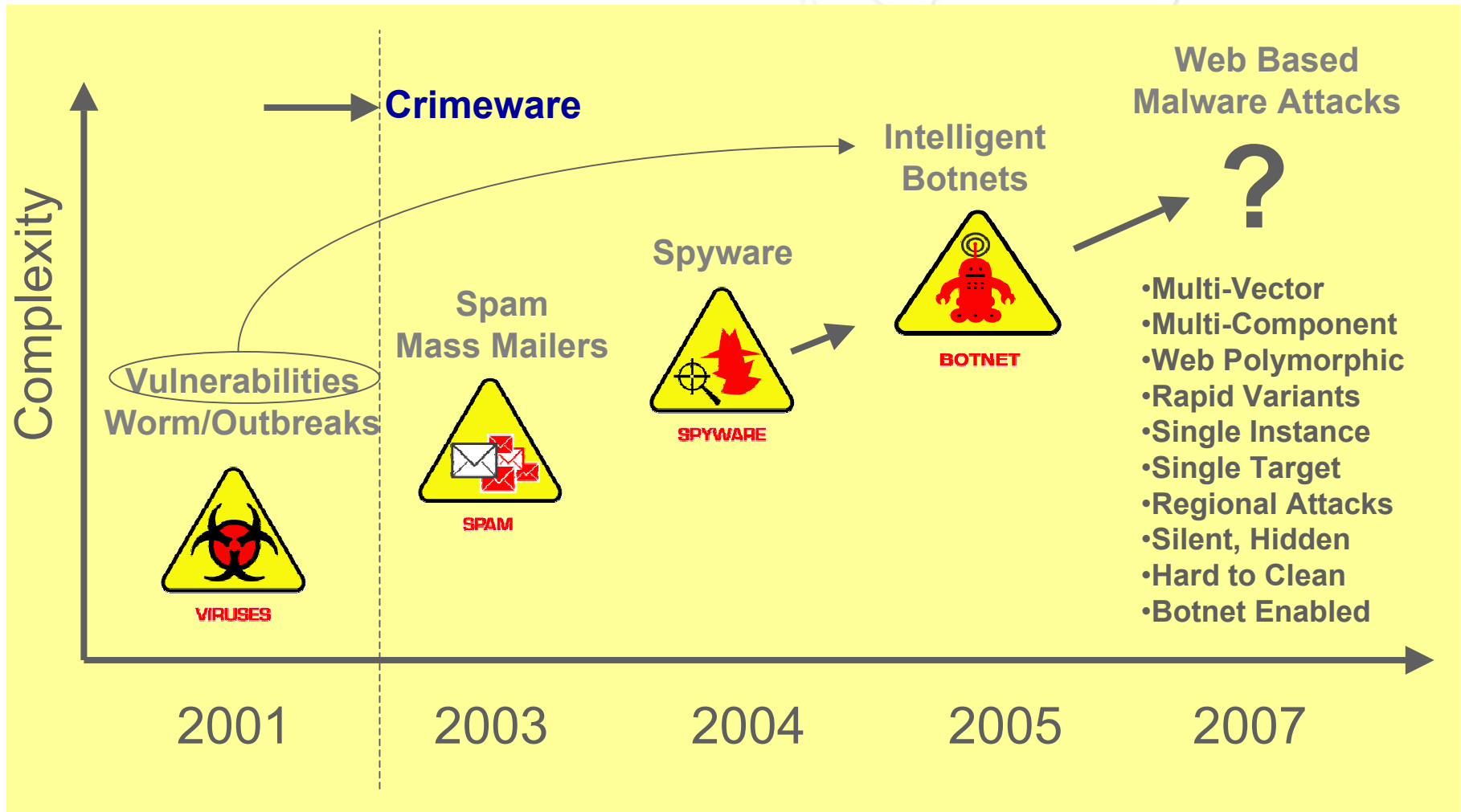
Securing Your Web World



THE RISE OF THE WEB THREATS

MONEY CHANGES EVERYTHING...

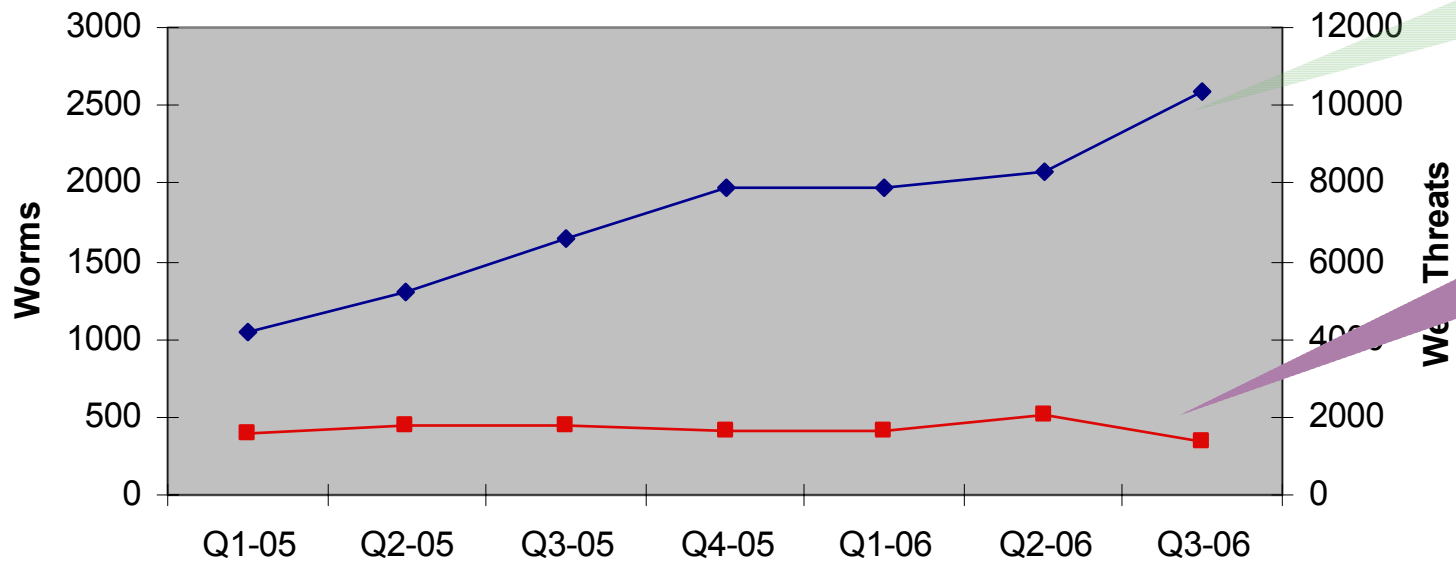
Threat Environment Evolution



Malware for Profit is driving Web Threats

The threat landscape is shifting to Web-borne attacks

Worms vs. Web Threats



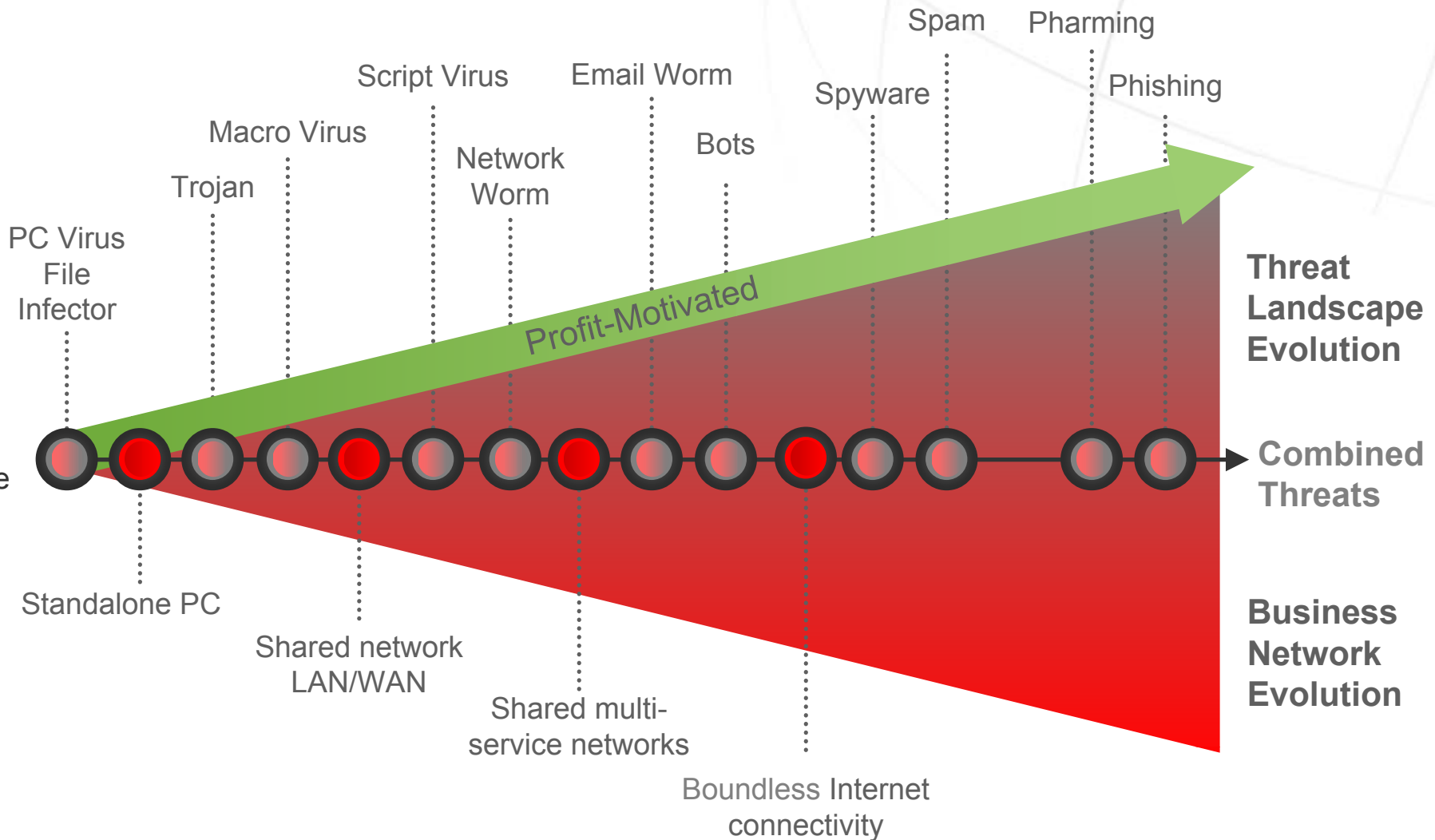
Web Threats:
High Volume
and Growing

Worms:
Constant in the
last 2 years

Source: Trend Micro

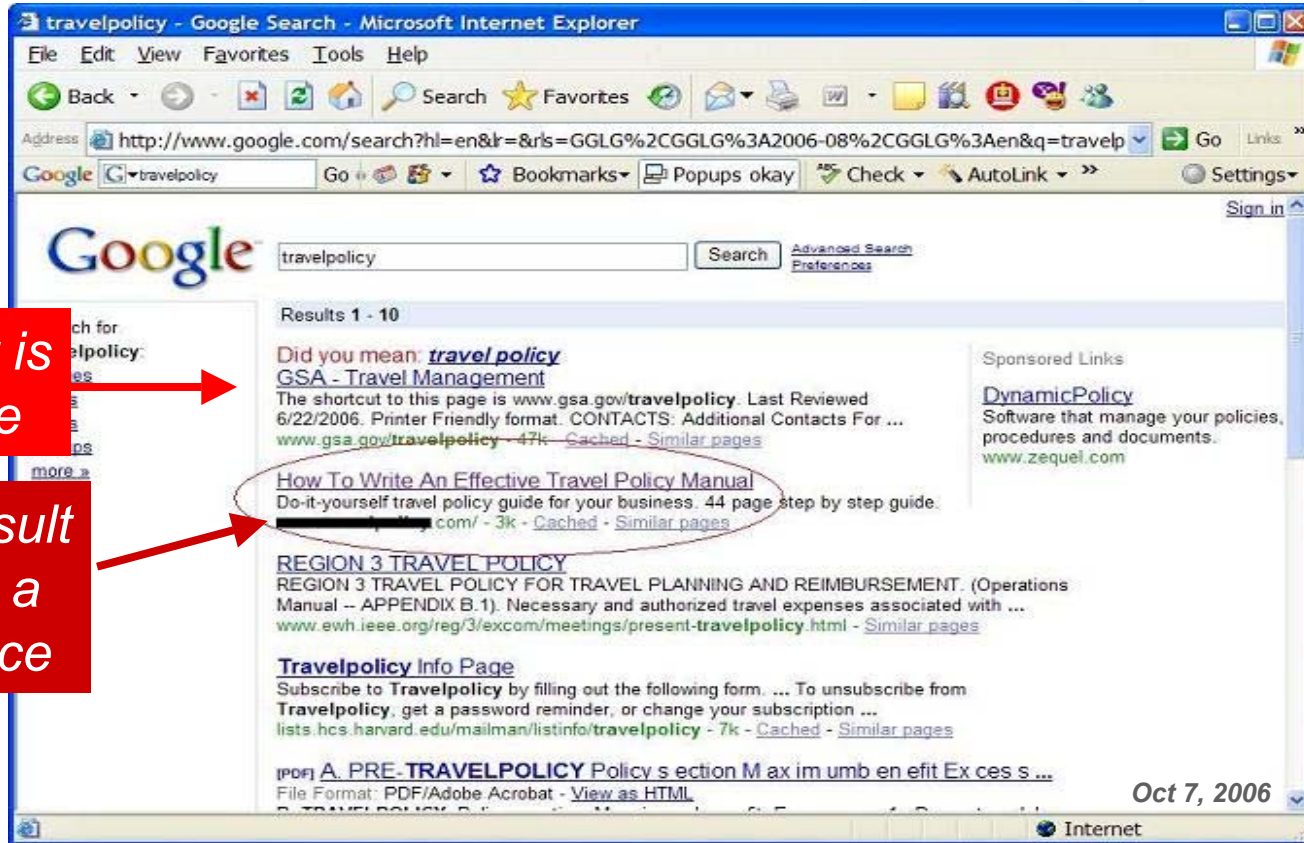
The Problem

Threat Landscape Is Evolving



Haxdoor

- ① Your boss asks you to develop a corporate travel policy
- ② You begin with a Google search on travel policy

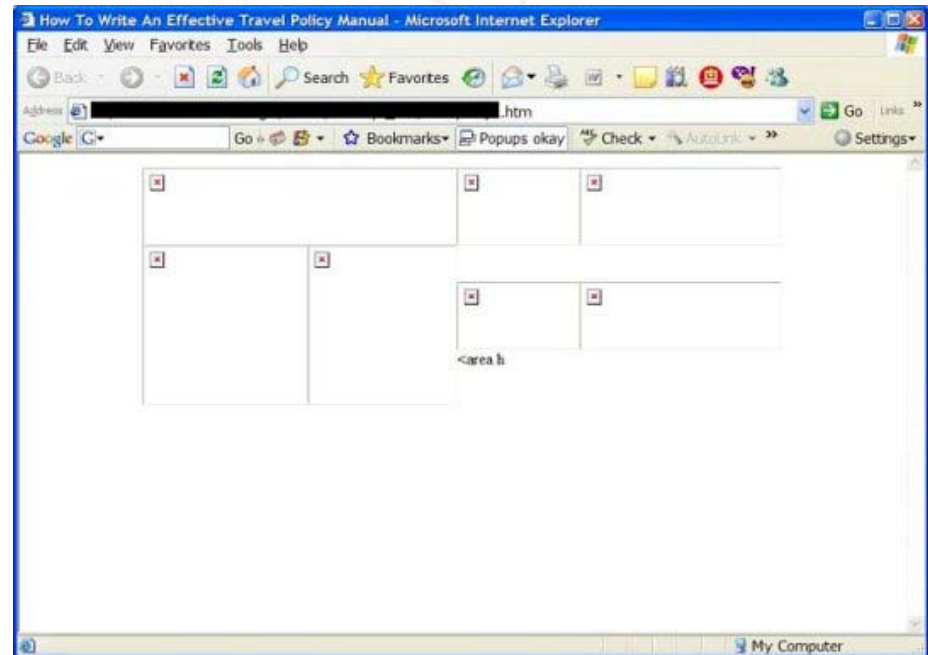


First result is a .gov site

Second result looks like a good choice

Haxdoor

- ① You click on the second search result
- ② You wait...the site appears to be downloading images and content...you wait...and you wait...
- ③ Finally you close the browser window...you'll find another site



Unbeknownst to you...

- The IFRAME at the top of the page leads you to an index.htm file (81.95.146.98/index.html)
- This file includes a script that exploits the **MS Internet Explorer (MDAC) Remote Code Execution Exploit (MS06-014)**
 - The original exploit code has been modified to try to bypass AV scanners that detect the original exploit
- An executable file (win.exe) is downloaded to your system and executed
- You now have a backdoor with rootkit features—a variant of the notorious family of backdoor rootkits known as **Haxdoor!**

ZLOB on myspace!

Securing Your Web World

www.myspace.com/daav0 - Mozilla Firefox

File Edit View History Bookmarks Tools Help


http://www.myspace.com/daav0

Getting Started Latest Headlines

Home | Browse | Search | Invite | Film | Mail | Blog | Favourites | Forum | Groups | Events | Videos | Music | Comedy | Classifieds

daav0

"The MEME is the Virus of the Mind."



Male
52 years old
Huntington Beach,
California
United States

Last Login:
15/04/2007

View My: [Pics](#) | [Videos](#)

Contacting daav0

| | |
|-----------------|-------------------|
| Send Message | Forward to Friend |
| Add to Friends | Add to Favorites |
| Instant Message | Block User |
| Add to Group | Rank User |

MySpace URL:
<http://www.myspace.com/daav0>

daav0 is in your extended network

daav0's Latest Blog Entry [[Subscribe to this Blog](#)]

Wireless Security (San Francisco Chronicle) ([view more](#))

Happy Michelangelo Day! ([view more](#))

My professional bio ([view more](#))

Lindora Medical Weight Loss Clinic ([view more](#))

Grammys will lead to viruses! ([view more](#))

[[View All Blog Entries](#)]

daav0's Blurbs

About me:
I am 52 years old and live in Huntington Beach, California home town. I am happily married and grow my own 1 peppers and oranges and lemons. I play the banjo, guitar keyboards, (but not very well). I do magic (and by the way the four of clubs) also not very well. I love life, and I

Who are these women? Why do they want to be my friend?

Securing Your Web World

MySpace.com - Friend Request Manager - Mozilla Firefox

Edit View History Bookmarks Tools Help

Customize Links Free Hotmail Windows Marketplace Windows Media Windows

TrendProtect

MySpace.com | Help | SignOut

MySpace | People | Web | Music | Music Videos | Blogs | Video | Events

Search

powered by Google

Home | Browse | Search | Invite | Film | Mail | Blog | Favorites | Forum | Groups | Events | Videos | Music | Comedy | Classifieds

Mail Center Friend Request Manager

Approve or Deny Your Friend Requests [Help]

- Inbox
- Saved
- Sent
- Trash
- Bulletin
- Address Book
- Friend Requests **NEW!**
- Pending Requests
- Event Invites

Listing 1-2 of 2

1 of 1

| | Date: | From: | Confirmation: |
|-------------------------------------|-----------------------|---|---|
| <input checked="" type="checkbox"/> | Mar 23, 2007 2:07 PM |  | <p>Lia wants to be your friend!</p> <p>Approve Deny Send Message</p> |
| <input type="checkbox"/> | Mar 23, 2007 12:18 PM |  | <p>Celine wants to be your friend!</p> <p>Approve Deny Send Message</p> |

Listing 1-2 of 2

1 of 1

Select / Deselect All

Approve Selected Deny Selected

Approve or Deny your selection

Sponsored Links

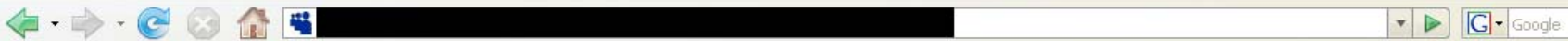
Free AOL® Email Account

Get Ringtones Now

Whence springs the trap

www.myspace.com/171111975 - Mozilla Firefox

File Edit View History Bookmarks Tools Help



Customize Links Free Hotmail Windows Marketplace Windows Media Windows

TrendProtect



This profile contains adult content.
CLICK HERE to install MS Viewer.

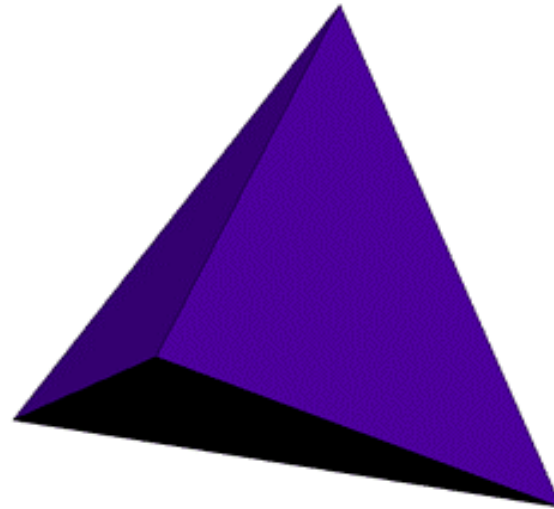
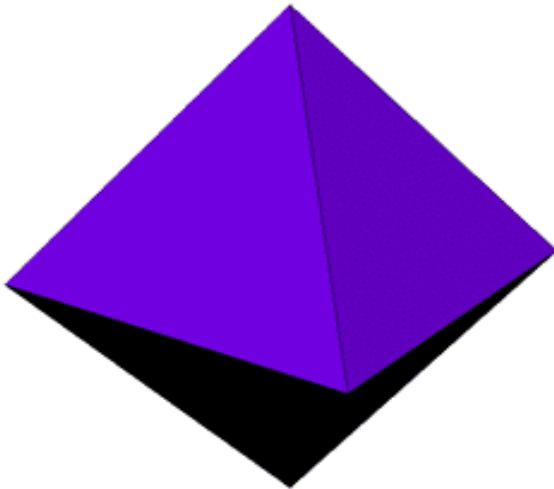
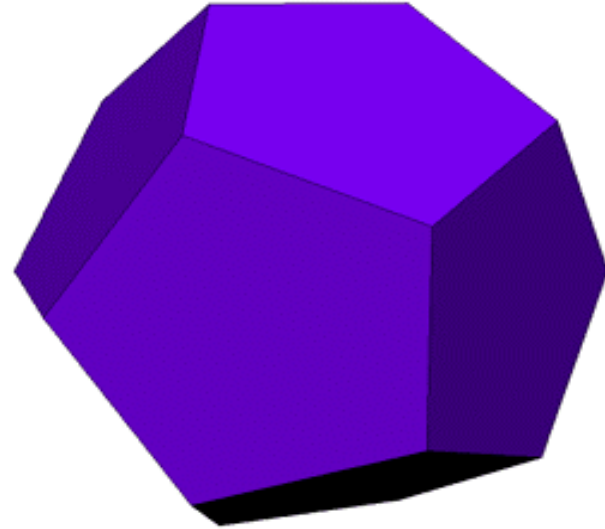
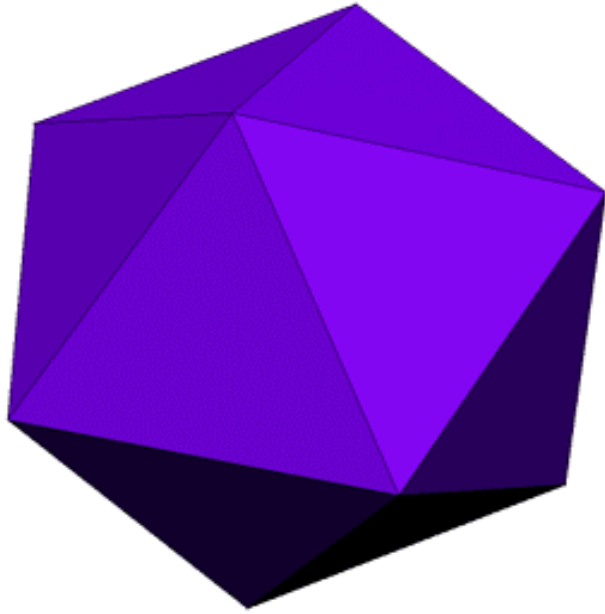
fieds



tha
folks
rest



Many Facets to identify



Four components of Web Threats

| <i>How does it get there?</i> | <i>What does it do?</i> | <i>How does it do it?</i> | <i>How does it protect itself?</i> |
|--|--|--|---|
| installed by: | money from: | operates by: | protected by: |
| <ul style="list-style-type: none"> ▪ Exploit ▪ unknowing consent ▪ lack full disclosure ▪ Freeloader ▪ Trojan ▪ Worm | <ul style="list-style-type: none"> ▪ Adware ▪ trackware ▪ keylogger ▪ browser hijacker ▪ fraudulent changes ▪ fraudulent royalty | <ul style="list-style-type: none"> ▪ BHO ▪ toolbar ▪ LSP ▪ application ▪ cookie ▪ Dialer | <ul style="list-style-type: none"> ▪ Rootkit ▪ watchdog program ▪ mimicry ▪ Polymorphic |

One web threat explored...

Example: Integrated Search Technologies (ISTBar)

| How does it get there? | What does it do? | How does it do it? | How does it protect itself? |
|--|---|---|--|
| installed by: | money from: | operates by: | protected by: |
| ActiveX- using social engineering to piggyback on installation of mp3 downloads, game cheats, song lyrics, porn, etc. | Collecting pay-per-click and other money from online advertisers for serving pop-up ads on infected PCs. | Toolbar, search companion, and homepage redirect | Unprotected – uses normal uninstaller supplied by publisher |

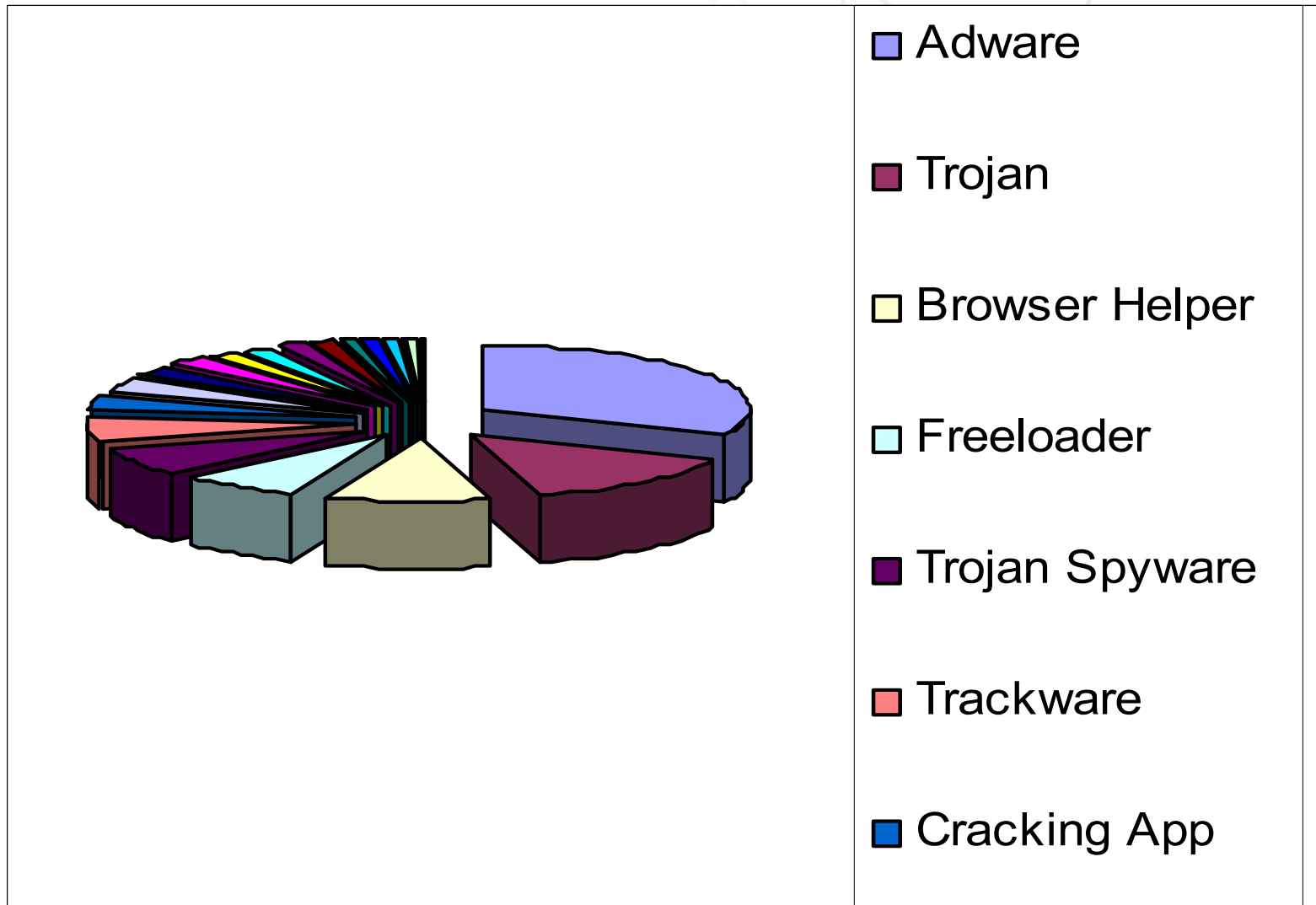
Problems of scale...

- Sometimes getting too close to an object obscures its place in the greater scheme...



- Double Fraud
- Silent installation
- Stealth *persistence!*
- *Malware self-defense*
- *Vertical segmentation*

Types of web threats by number of infected systems...



***(definable)* Facets of a web threat**

- **How does it get on to the victim's computer? (method of access)**
- **What unwanted activities does it perform on the victim's computer? (economic purpose)**
- **How does it technically accomplish its purpose? (method of accomplishment)**
- **How does it protect itself from being detected, blocked or removed? (self-defense)**

- Is this already too complicated for the end user to understand?
- Unfortunately, it won't work (beat you to it, vess)

- **We don't call a bank robbery by the weapon**
- **We don't normally hide that a crime has taken place**
- **Jurisdiction is clearer**
- **The public and the experts share a *gestalt* on the nature of most crimes**

Big concept, little time, conclusions

- **The ultimate purpose of any digital threat categorization system is to provide clear, actionable information that allows everyone (from anti-malware product designers to IT administrators to individual PC users) to make prudent, effective cost/risk security decisions.**
- **The shift in malware from vandalism to monetary gain suggests that economic purpose rather than technical method of exploitation be the primary consideration in threat classification.**
- **Economically-motivated threats typically possess multiple functional aspects (e.g., installation, money-making, self-preservation) requiring multi-dimensional categorization.**

Thank you, *please read the paper!*



And, of course, questions...

