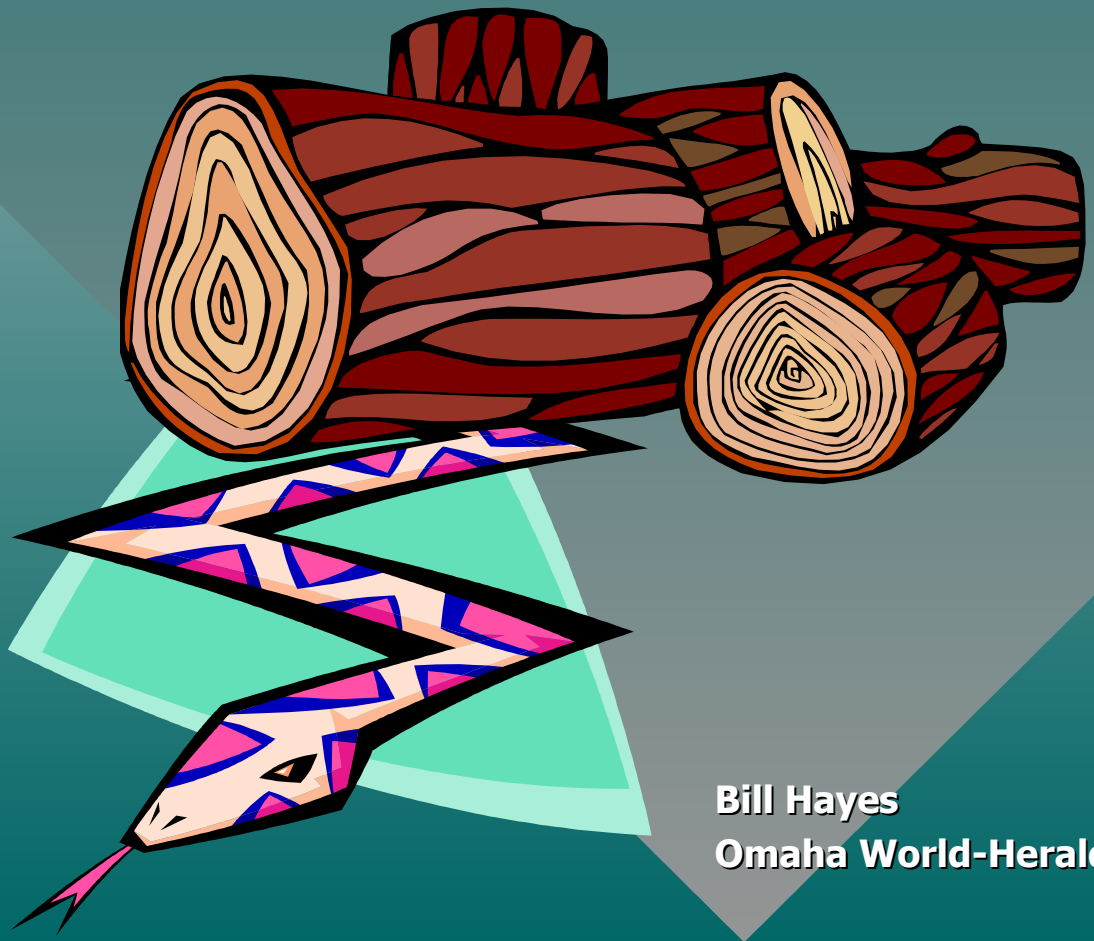
Snake in the woodpile - Spyware in your PCs



Bill Hayes
Omaha World-Herald Company

Introduction

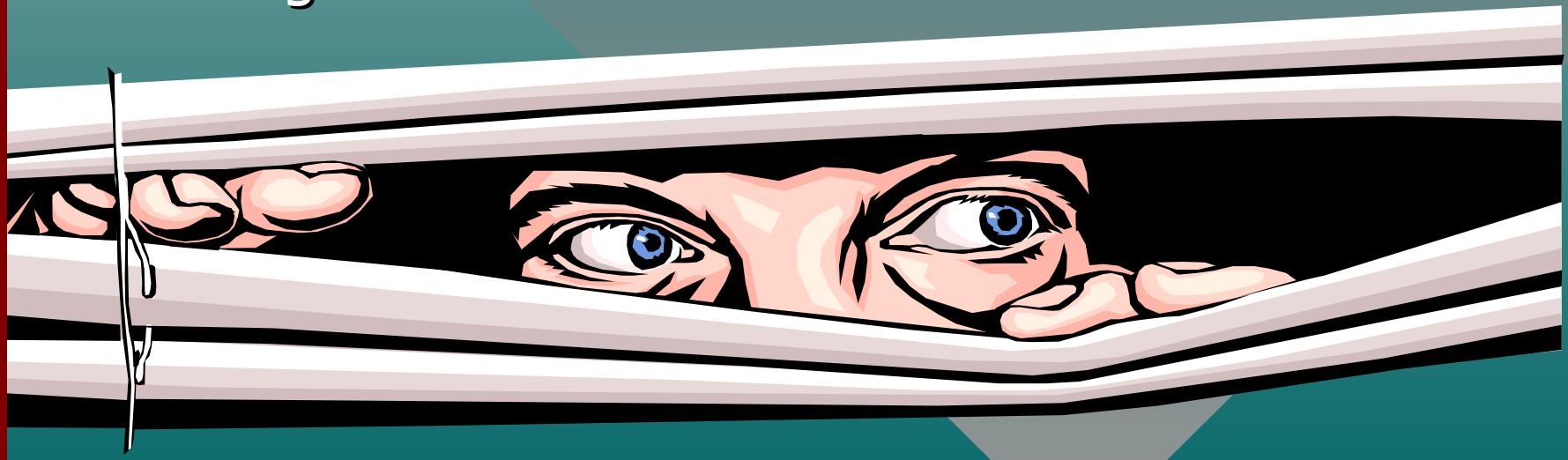
Spyware is a toxic form of unsolicited for-profit software that threatens the confidentiality, integrity, and availability of computer systems and their data.

Introduction continued

In this presentation we will discuss how spyware is propagated and how it can be detected and eliminated using multiple levels of defense.

Spyware is widespread

Some 2003 estimates claim infestation ranges as high as 91% for all home broadband Windows PCs. In Q1 2005, Webroot reported 88% of all home PCs had spyware with 7.2 instances per machine, not counting tracking cookies.



Sources - National CyberSecurity Alliance, Webroot

Spyware threatens commerce

Webroot claims 55% infection rate for business machines, not counting tracking cookies. In late July, FDIC issued spyware protection guidelines.

Source - Webroot, Reuters July 22, 2005

Spyware - What is it?

Currently, each anti-spyware vendor has its own naming convention and terminology. We'll first cover the confusing spyware terms and propose a better definition of spyware.

What is Spyware?

- Anti-spyware vendors and end-users often label all undesired software that isn't a virus as spyware.
- Spyware is less often called "grayware", "unsolicited commercial software" or "potentially unwanted programs" (PUPs).

Spyware by characteristic

Spyware reports user action to an outside source without the user's knowledge. It may redirect surfing through a proxy, steal cookies, or report user URLs.

Spyware characteristics continued

Spyware is installed through deception and is often completely undetected by the user. If a EULA is displayed, terms are misleading or obscured.

Spyware characteristics continued

The purveyors of spyware exploit infested platforms for monetary gain.

Spyware is principally used to retrieve personal information useful to marketing firms and to present advertising to the users of an infested computer.

A Better Spyware Definition

Spyware is a for-profit product, distributed through misdirection, and managed by a business venture. Usually intended for marketing research, it can also be used for industrial or national espionage.

Spyware types

Dialers - dials "900" numbers without user's knowledge. These are frequently associated with porn sites. Often found on the same system with other forms of spyware.

Spyware types continued

Downloaders - Used to download spyware or adware usually without user knowledge. Used in "drive-by" installation attempts. One downloader can install a number of different spyware progams.

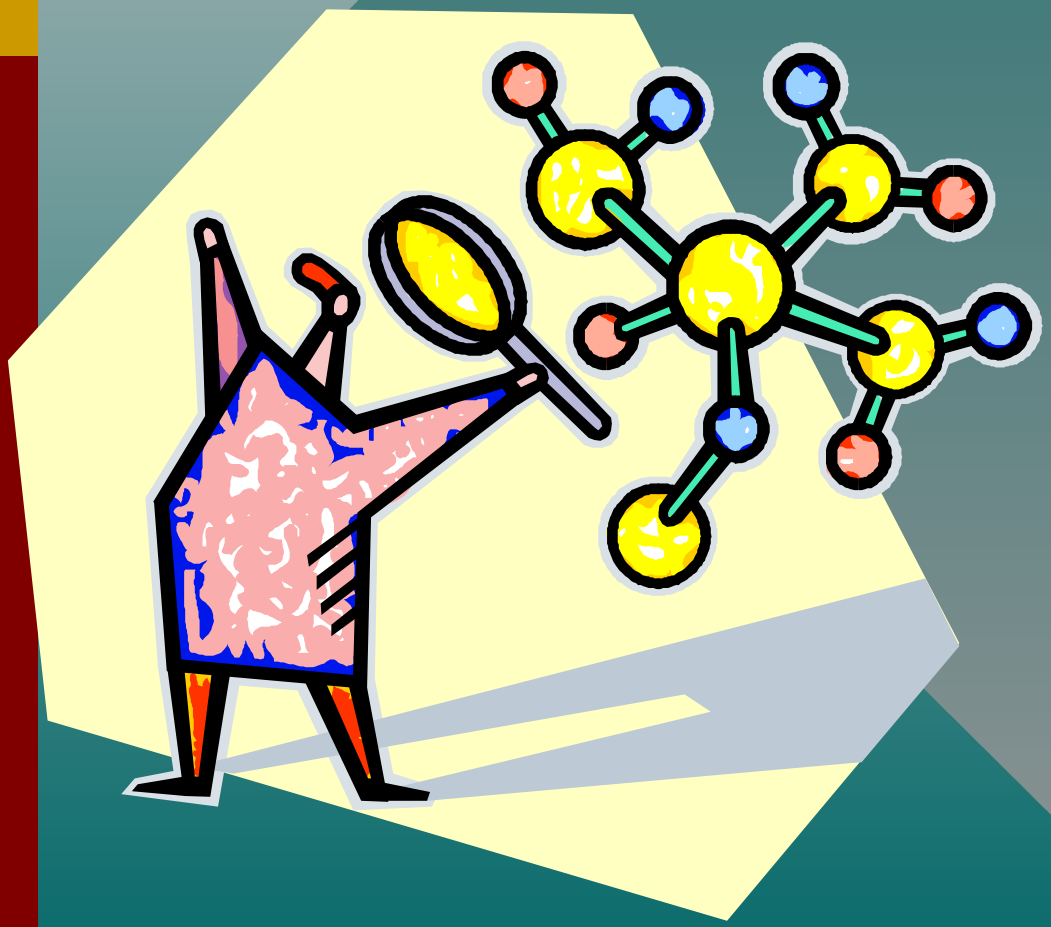
Spyware types

- Adware - displays ads or redirects Internet searches to sites displaying client information.
- Spyware - Collects information on user and/or programs then reports to controlling site.

Spyware types continued

Tracking Cookie - stores information about user's surfing activity and shared by two or more sites. Could be privacy threat. Could be exploited by other malware.

Spyware components



- Browser Helper Object (BHO)
  - hard to detect
- Toolbar
  - found with BHOs
- Ad display
  - Popups
  - Banners
- Search Redirectors

Spyware purveyors

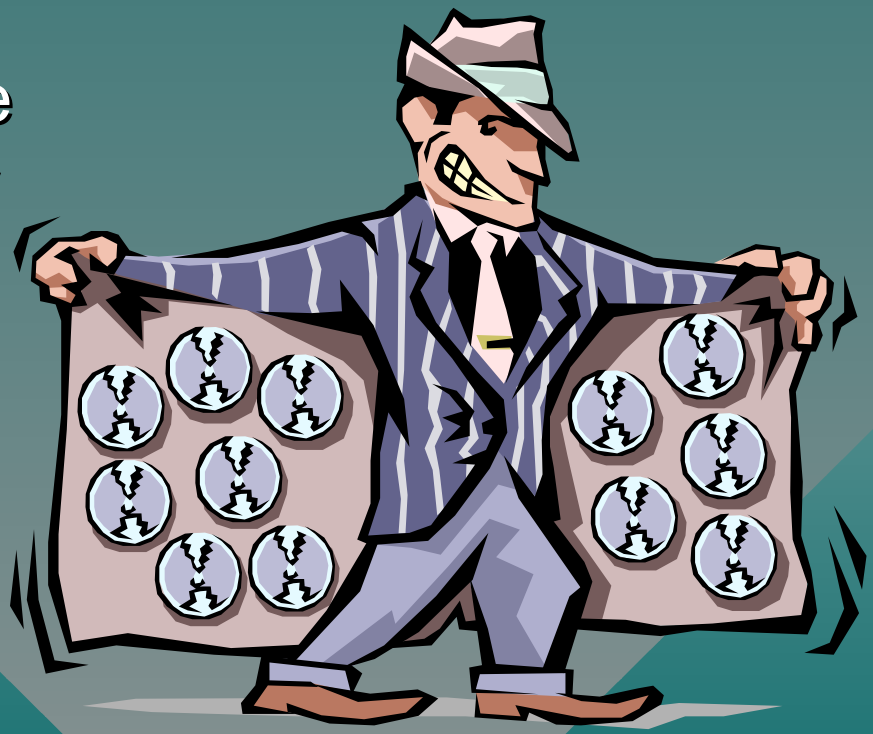
Spyware purveyors profit by being the middle men between users and the services they access. They may enlist the help of affiliates to distribute their software.

Spyware distribution channels

Spyware distribution channels include software bundling, through affiliate web sites, or less often through spam. Spyware has often been bundled with shareware or with Peer-to-Peer software.

Spyware Affiliate Sites

Spyware affiliate sites earn money by helping spyware companies download their software to end user computers. Webroot claims there are 250,000 web pages worldwide that can download spyware.



Spyware Affiliate Sites continued

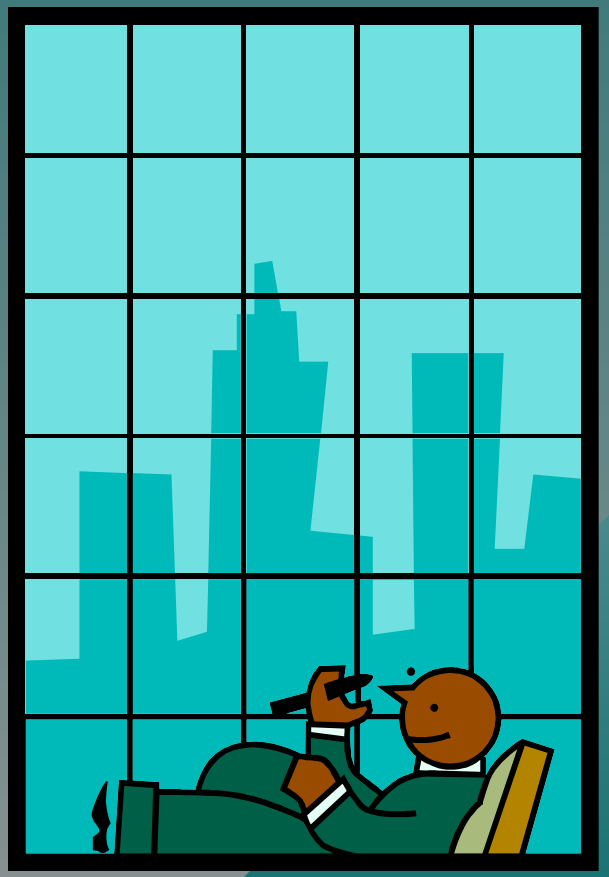
Unscrupulous affiliates exploit Internet browser flaws in “driveby” installation attempts, often through compromised sites. Users are usually unaware of the installation attempts.

Bundled Spyware

Spyware can be bundled with shareware or Peer-to-Peer file sharing programs. Gator (Claria) has been successfully distributed this way.

Top Spyware Purveyors ranked by investment capital*

- Intermix (KeenValue) - $102 million
- Claria (Gator) $58 million
- 180Solutions (nCase) $40 million
- BetterInternet, LLC (ABetterInternet) $20 million
- eXact Advertising (BargainBuddy) $15 million



* Sources - http://www.benedelman.org, http://finance.yahoo.com/q/it?s=MIX

Top Spyware Purveyors ranked by spyware detections in the past 6 months*

- Gator (Claria)
- ABetterInternet (BetterInternet, LLC)
- Huntbar (First Cash Reserve, LLC)
- Hotbar (Hotbar.com Inc.)
- ISTBar (Integrated Search Technologies)

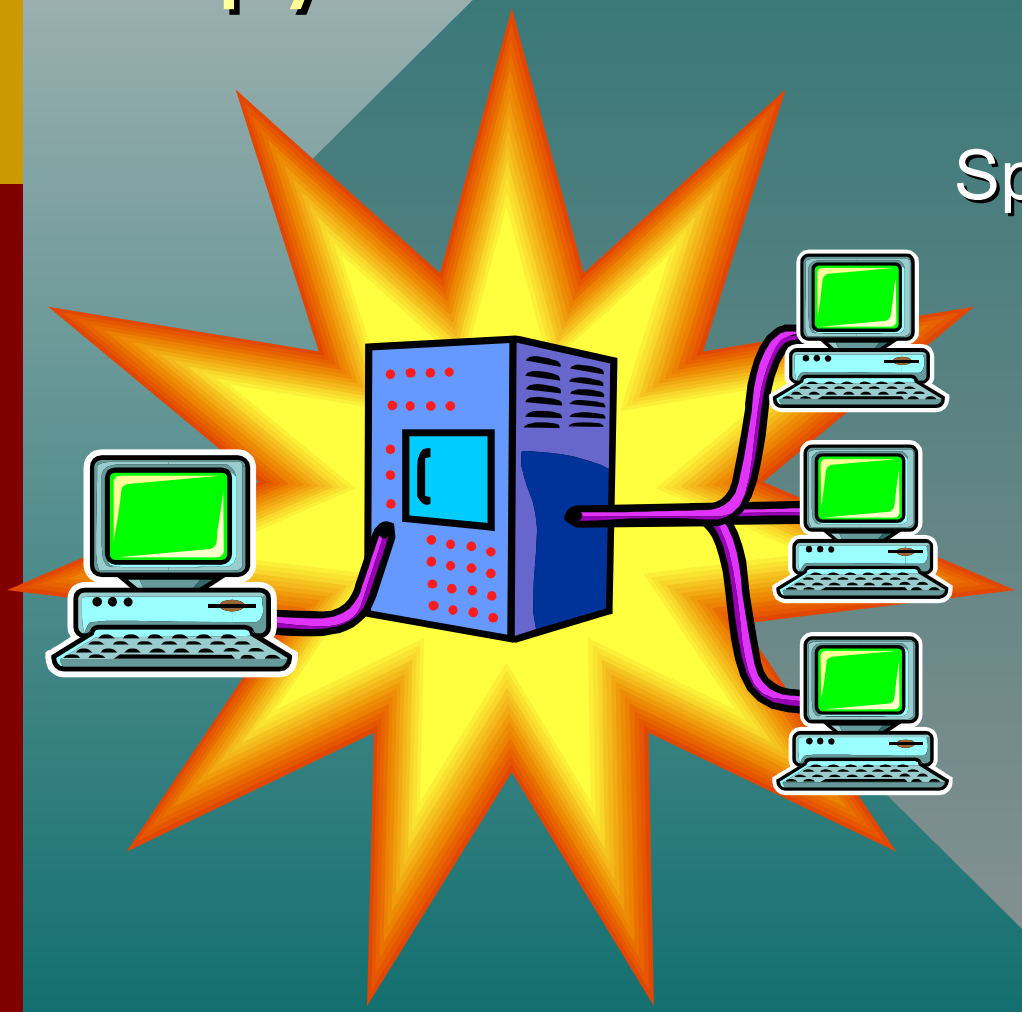
* Sources - NAI, Panda, PestPatrol, SpywareGuide, and TrendMicro. Ranked by Bill Hayes

Top Spyware Purveyor in Eastern Europe*

CoolWebSearch - A Russian spyware firm. Has many affiliates associated with independent operators. These relationships are sources for many Trojan horses that bundle malware and spyware. Over 70 CWS variants.

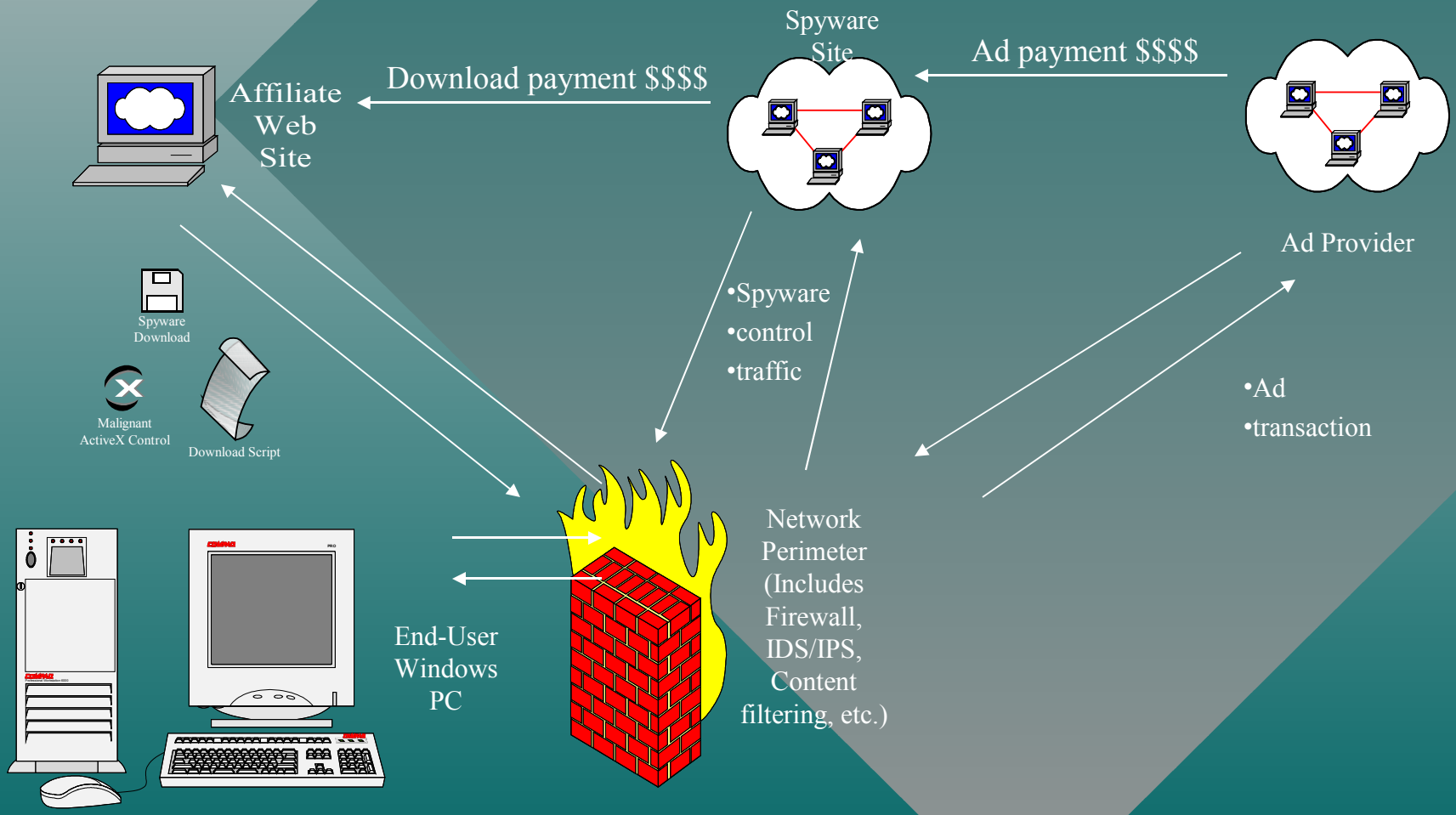
* Sources - DoxDesk, Merijin.org, PestPatrol, Webroot

Spyware servers



Spyware servers can download spyware to “client” hosts. They then control spyware client sofware. Additionally, they may also offer advertising content.

Spyware servers



Simplified block diagram showing Affiliate - Spyware/Adware Site - Ad Site relationships

Spyware Detection

The bad news - No single tool can yet detect all spyware.

The good news - Defense in Depth still works once you adapt to new detection strategies.

Spyware Defense Strategy

- Block spyware download attempts
- Block access to known spyware sites
- Correlate logs to identify new threats
- Provide spyware recognition training

Block spyware downloads

- Use IDS/IPS to deal with download sites
- Bleeding Edge of Snort resources (http://www.bleedingsnort.com/)
- Use web proxy AV

  Open source and proprietary solutions

  Open source - ClamAV (http://www.clamav.net/)

  Proprietary - See your favorite VAR!

Block known spyware sites

- Network Based solutions

  Use web content management software

  DNS realtime blocking list for spyware
  http://www.bleedingsnort.com/blackhole-dns/

Block known spyware sites continued

- Anti-Virus/Anti-Spyware software

  Note: No single program detects everything

- Custom Hosts files

  Note: Can have 10, 000 or more hosts. Can be used on older boxes.

- Place download IP addresses in IE Restricted sites list

Analyze & correlate log files

Spyware has definite characteristics

- It phones home regularly to predictable hosts (may only be IP addresses).
- Logs will show repeatable patterns.
- Look for activity especially when users have logged off.
- POST http method may show communication with controller host, but many spyware progams use GET http method with user QUERY parameter fields to transmit data.

Examples

MarketScore -

GET http://oss-survey.marketscore.com/oss/survey.asp ?numdays=49

HotBar - POST http://reports.hotbar.com/reports/hotbar/4.0/HbRpt.dll

Analyze & correlate log files continued

Correlate AV, web proxy, and IDS logs

- Eyeball logs - Ouch!
- Consolidate logs then use scripts - Less painful.
- Use proprietary solution - Buck$ but less labor-intensive

Analyze findings

- There's no substitute for brain power.

Create and distribute meaningful reports

Spyware recognition training

Train end users to report spyware manifestations immediately

- Ad pop-ups
- new browser toolbars
- home page changes
- desktop changes
- Systray icons

Spyware recognition training

- Train support personnel to recognize spyware installers.
  - Don’t just run AV scan and call it quits. Look it up!
- Train IDS/Content Management analysts to recognize spyware activity.
  - Spyware activity is often revealed by other attack signatures.

Conclusion

- Spyware is a threat to the confidentiality, integrity, and availability of computer systems and data.
- Technology for accurate spyware detection is still developing.
- Defense in Depth with modifications can mitigate spyware risks.

References

Research References

http://www.doxdesk.com/parasites

http://www.benedelman.org

http://www.spywareinfo.com/~merijn/cwschronicles.html

http://www.webhelper4u.com/

Technical References

http://castlecops.com

http://www.bleedingsnort.com/bleeding-malware.rules

http://www.mvps.org/winhelp2002/hosts.htm

http://www.mvps.org/winhelp2002/restricted.htm

http://www.spywareguide.com/blockfile.php

References

Spyware Encyclopedias

http://www.doxdesk.com/parasites

http://www3.ca.com/securityadvisor/pest/

http://www.kephyr.com

http://www.spywareguide.com/

AV/Spyware Encyclopedias

http://securityresponse.symantec.com/avcenter/

http://www.trendmicro.com/vinfo/grayware/default.asp

http://www.pandasoftware.com/virus_info/default.aspx?lst=sw

http://vil.nai.com/vil/

Anti-Spyware Software

Freeware

SpyBot S & D - http://www.safer-networking.org/en/index.html

HiJackThis - http://www.spywareinfo.com/~merijn/downloads.html

IESPYAD - https://netfiles.uiuc.edu/ehowes/www/resource.htm

Shareware

Ad-Aware - http://www.lavasoft.com/

Some commercial anti-spyware products (not an endorsement)

Microsoft Antispyware - http://www.microsoft.com/athome/security/spyware/

PestPatrol - http://www3.ca.com/smb/product.aspx?id=5277&culture=en-us

Spy Sweeper - http://www.webroot.com