Snake in the woodpile - Spyware
Countermeasures for the Enterprise

Bill Hayes
Omaha World-Herald Company
Spyware is a toxic form of unsolicited for-profit software that threatens the confidentiality, integrity, and availability of computer systems and their data.
In this presentation we will discuss how spyware 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 Q2 2005, Webroot reported 80% of all home PCs had spyware, not counting tracking cookies.

Sources - National CyberSecurity Alliance, Webroot
Spyware threatens commerce

Webroot claims 80% infection rate for business machines in Q2 (up from 55%), not counting tracking cookies. In late July, FDIC issued spyware protection guidelines.

Source - Webroot, Reuters July 22, 2005
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 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 over 300,000 web pages worldwide that can download spyware (up from 250,000 in Q1).
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.
Spyware can be bundled with shareware or Peer-to-Peer file sharing programs. Gator (Claria) has been successfully distributed this way.
Spyware servers can download spyware to “client” hosts. They then control spyware client software. 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**
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 programs use GET http method with user QUERY parameter fields to transmit data.

Examples

MarketScore -

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/
http://virusbtn.com/
http://sunbeltblog.blogspot.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://vil.nai.com/vil/
Anti-Spyware Software

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

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

Some commercial anti-spyware products (not an endorsement)
CounterSpy - http://www.sunbelt-software.com
Spy Sweeper - http://www.webroot.com