

# Snake in the woodpile - Spyware and Targeted Attacks



Bill Hayes, CISSP  
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

Targeted attacks are focused attacks against a particular organization. Victims are chosen to maximize the effectiveness of the attacks.



# Introduction continued



In this presentation we will discuss how spyware used in targeted attacks can be detected and eliminated using multiple levels of defense.

# Spyware is still widespread

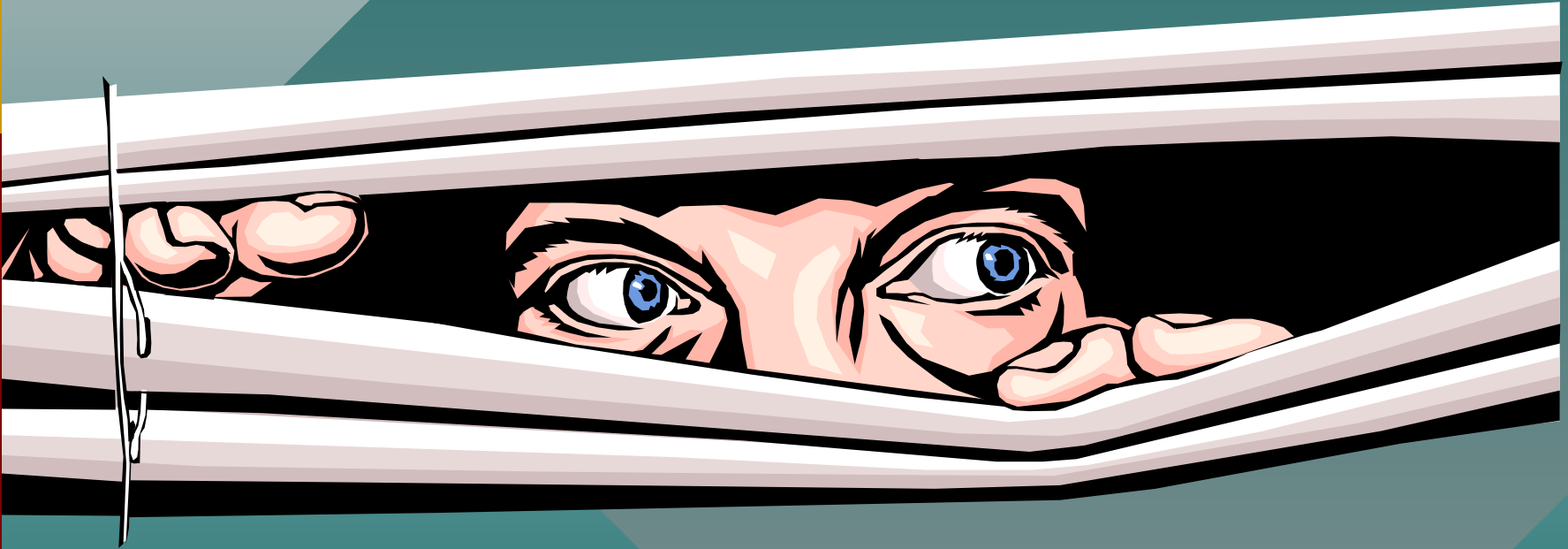
Harvard spyware researcher Ben Edelman says that despite recent government action such as the FTC suits, spyware purveyors are still up to their old tricks.

On June 13th, 2007, the FTC warns of spyware-laden spam supposedly from the FTC!



Sources - Ben Edelman ([www.benedelman.org](http://www.benedelman.org)), Federal Trade Commission

# Spyware Threatens Commerce



Webroot claims over 80% infection rate for business machines surveyed in 2006, not counting tracking cookies.

Source: Webroot Q1 2007 *State of the Internet* report

# Targeted Attacks Are Growing

Webroot claims 39 percent enterprises surveyed in January of 2007 dealt with Trojan horse attacks and 24 percent with system monitor (keylogger) attacks.

July 2007 “Ransomware” targeted attacks net victims in Fortune 500 and US government agencies.



Source: Webroot Q3 2007 *State of the Internet* page

# A Better Spyware Definition



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

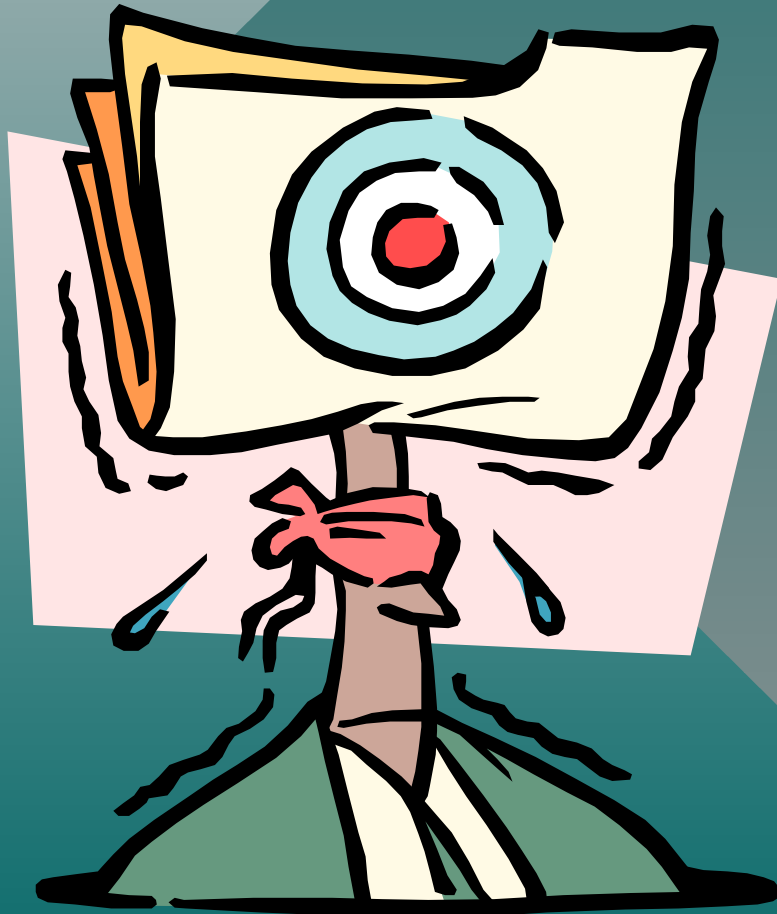


# Spyware Purveyors

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.



# Targeted Attackers



Targeted attackers use focused and illegal means to distribute spyware to victims within targeted organizations. Their goal is access to valuable data or to deny user access to valuable data.

# 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 (P2P) software.



# Targeted Attack Methods

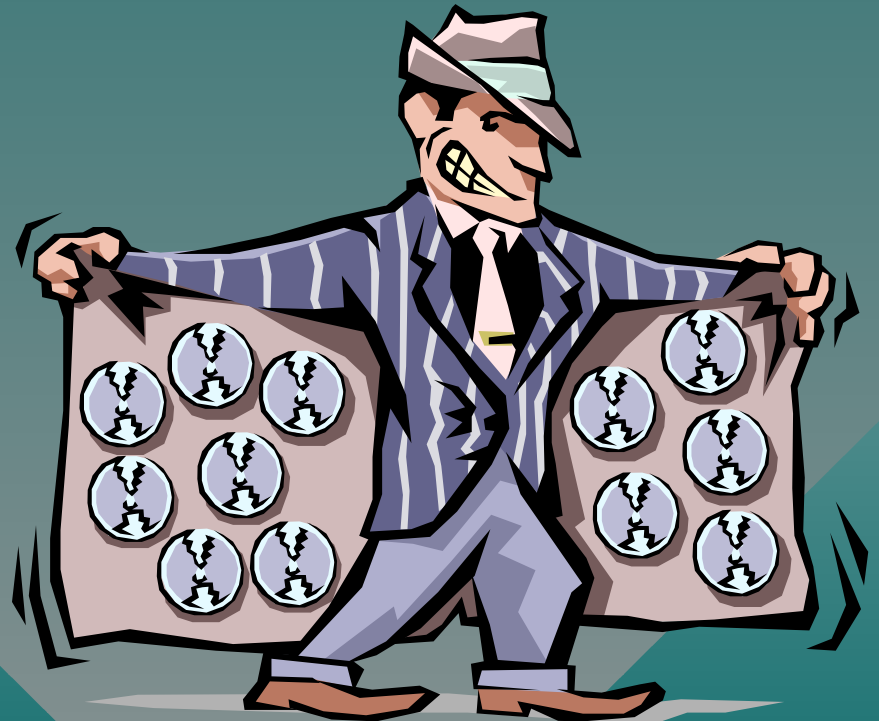


Targeted attack channels include software bundling, spear phishing, or less often through compromised web sites.

Targeted attack malware can also be delivered through compromised software media or USB memory sticks.

# Spyware Affiliate Sites

Spyware affiliate sites earn money by helping spyware companies download their software to end user computers. In its Q1 2007 security report, Webroot claims there are now over 3,000,000 web pages worldwide that can download malware.



# Spyware Affiliate Sites continued



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

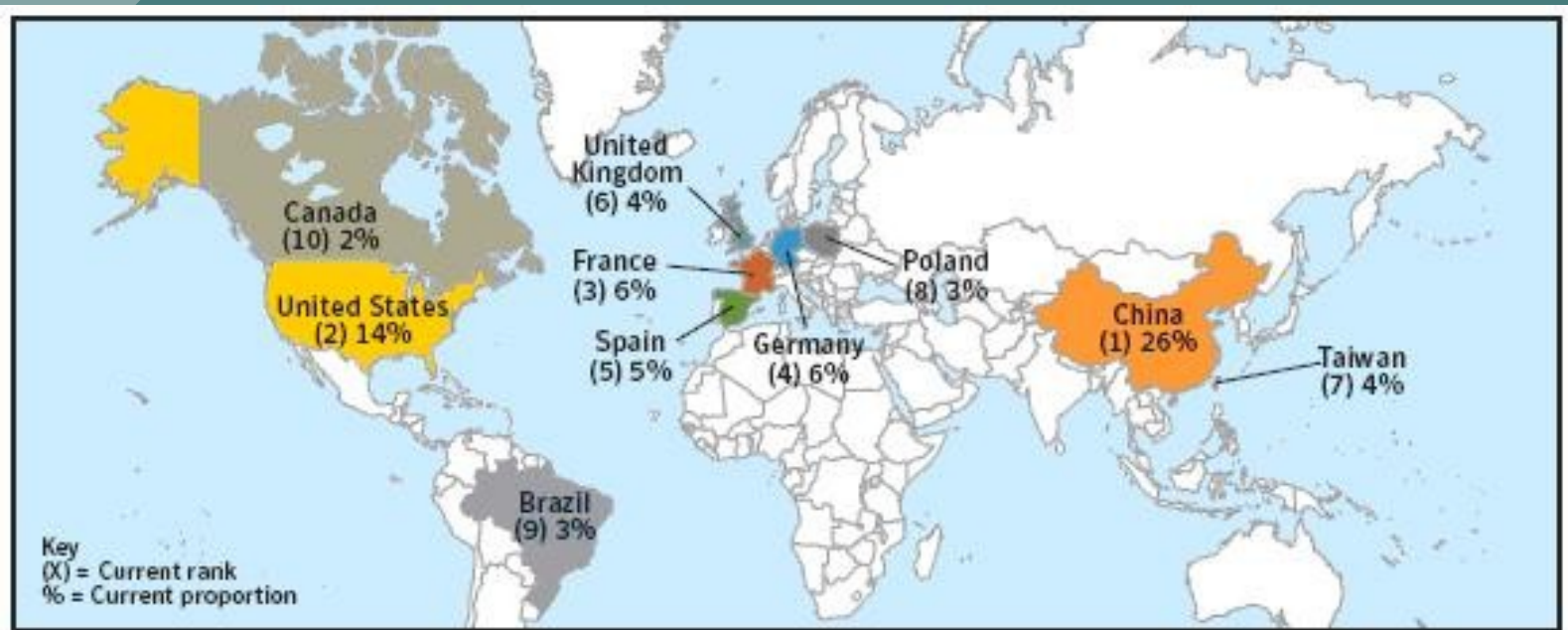
# Bundled Spyware



Spyware can be bundled with shareware or Peer-to-Peer (P2P) file sharing programs. Gator (Claria) has been successfully distributed this way.

# Botnets As Distribution Channels

Used to launch spam and spear phishing campaigns



Bot-infected computers by country

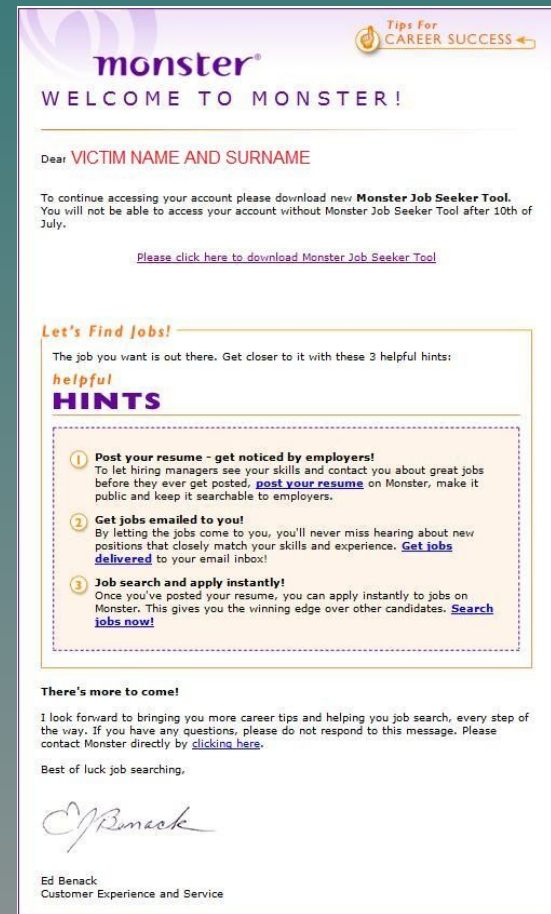
Source: Symantec Internet Security Threat Report Volume XI

Source: Symantec Security Response Blog



# Targeted Attack - Ransomware

In early July 2007, attackers now thought to be associated with Russian hackers known as the Russian Business Network (RBN) began targeted attacks against businesses and government agencies using a bogus “monster.com” message.



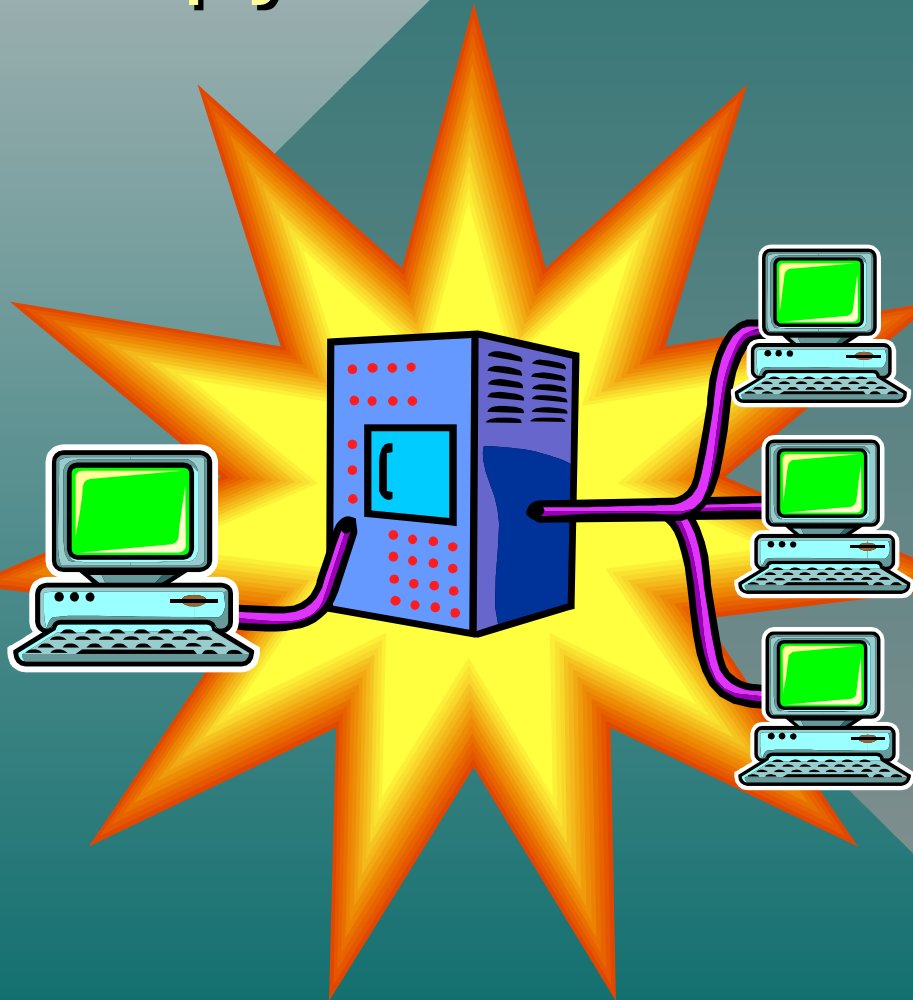
- Sources: Prevx.com, Kaspersky Labs

# Targeted Attack - Ransomware

"Hello, your files are encrypted with RSA-4096 algorithm (<http://en.wikipedia.org/wiki/RSA>). You will need at least few years to decrypt these files without our software. All your private information for last 3 months were collected and sent to us. To decrypt your files you need to buy our software. The price is \$300. To buy our software please contact us at: [tristanniglam@gmail.com](mailto:tristanniglam@gmail.com) and provide us your personal code -xxxxxxxxx. After successful purchase we will send your decrypting tool, and your private information will be deleted from our system. If you will not contact us until 07/15/2007 your private information will be shared and you will lost all your data -- Glamorous team."

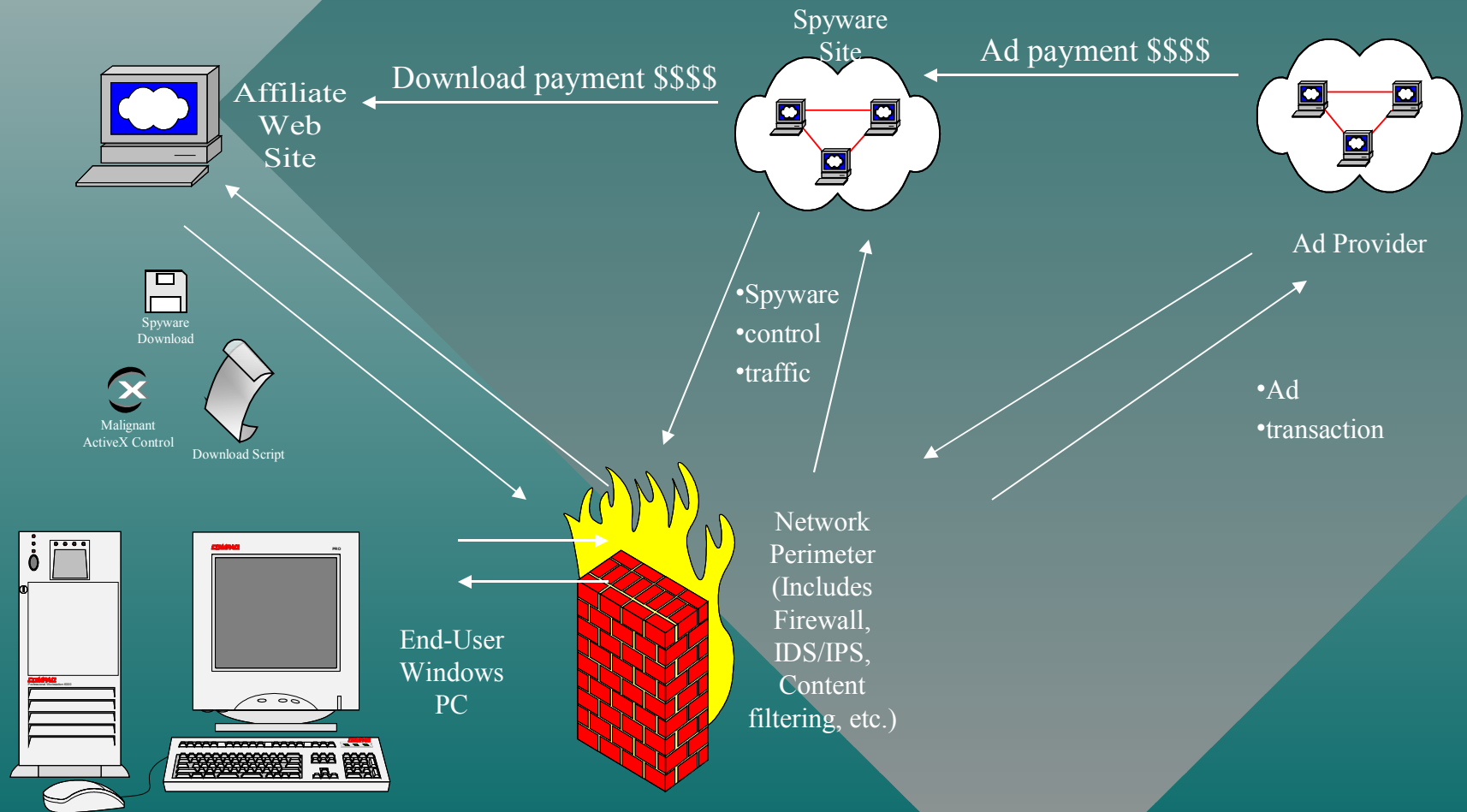
Source: [Prevx.com](http://Prevx.com)

# Spyware Servers



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

# Spyware Servers continued



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.




# Targeted Attack Detection



Targeted attacks are often difficult to detect because many security signature-based tools are not updated often enough and may not consider low-volume “tailored” attacks.

# July Ransomware Detection

July ransomware attacks were not immediately detected by many major AV vendors even with heuristics enabled. By July 13th, AntiVir, AVG, and F-Prot detected it. A Virustotal.com snapshot taken by Prevx showed more were able to detect it by the 14th. Finally, by July 17th, Symantec and McAfee respectively added detection as "Trojan.Grocer.F" and "Trojan.Grocer.F". Sources: Prevx.com, McAfee, Symantec.

File <b>ntos.ex_</b> received on <b>07.14.2007 17:08:46 (CET)</b>			
Current status: <b>finished</b>			
<a href="#">Print results</a> 			
Antivirus	Version	Last Update	Result
AhnLab-V3	2007.7.14.0	2007.07.14	no virus found
AntiVir	7.4.0.39	2007.07.13	TR/Crypt.XPACK.Gen
Authentium	4.93.8	2007.07.13	no virus found
Avast	4.7.997.0	2007.07.13	no virus found
AVG	7.5.0.476	2007.07.13	PSW.Generic4.XCV
BitDefender	7.2	2007.07.14	no virus found
CAI-QuickHeal	9.00	2007.07.14	(Suspicious) - DNAScan
ClamAV	devel-20070416	2007.07.14	no virus found
DrWeb	4.33	2007.07.14	no virus found
eSafe	7.0.15.0	2007.07.10	Suspicious Trojan/Worm
eTrust-Vet	30.8.3784	2007.07.14	no virus found
Ewido	4.0	2007.07.14	no virus found
FileAdvisor	1	2007.07.14	no virus found
Fortinet	2.91.0.0	2007.07.14	no virus found
F-Prot	4.3.2.48	2007.07.13	W32/new-malware!Maximus
Ikarus	T3.1.1.8	2007.07.14	Trojan-Downloader.Win32.Delf.aww
Kaspersky	4.0.2.24	2007.07.14	no virus found
McAfee	5074	2007.07.13	no virus found
Microsoft	1.2704	2007.07.14	Backdoor:Win32/Kollah.D
NOD32v2	2399	2007.07.14	a variant of Win32/Spy.Agent.FZ
Norman	5.80.02	2007.07.13	no virus found
Panda	9.0.0.4	2007.07.14	Suspicious file
Sophos	4.19.0	2007.07.06	no virus found
Sunbelt	2.2.907.0	2007.07.14	VIPRE.Suspicious
Symantec	10	2007.07.14	no virus found
TheHacker	6.1.6.146	2007.07.13	no virus found
VBA32	3.12.0.2	2007.07.13	no virus found
VirusBuster	4.3.23:9	2007.07.14	no virus found
Webwasher-Gateway	6.0.1	2007.07.14	Trojan.Crypt.XPACK.Gen

# 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 programs 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](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

Use sites like the FTC's [onguardonline.gov](http://onguardonline.gov) for refresher training

# Spyware Recognition Training

- Train support personnel to recognize spyware installers.
  - Don't just run AV scan and call it quits. Look it up!
  - Train first responders to preserve evidence for analysis.
- 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 and targeted attack risks.



# References

## Research References

<http://www.benedelman.org>

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

<http://www.webhelper4u.net/>

<http://virusbtn.com/>

<http://sunbeltblog.blogspot.com/>

<http://www.prevx.com/blog.asp>

[http://www.symantec.com/enterprise/security/security\\_response/weblog](http://www.symantec.com/enterprise/security/security_response/weblog)

<http://www.webroot.com/company/pressroom/pr/sois-07-q3.html>

## 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>

# References

## **Spyware Encyclopedias**

<http://www.ca.com/us/securityadvisor/pest/>

<http://www.kephyr.com/spywarescanner/library/index.phtml>

<http://www.spywareguide.com/>

[http://research.spysweeper.com/?id=H2-USEFUL\\_Links-TR](http://research.spysweeper.com/?id=H2-USEFUL_Links-TR)

## **AV/Spyware Encyclopedias**

[http://www.symantec.com/enterprise/security\\_response/index.jsp](http://www.symantec.com/enterprise/security_response/index.jsp)

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

[http://www.pandasoftware.com/virus\\_info/default.aspx?lst=sw](http://www.pandasoftware.com/virus_info/default.aspx?lst=sw)

<http://vil.nai.com/vil/>

## **End-User Training Resource**

<http://onguardonline.gov/stopthinkclick.html>

# Anti-Spyware Software

## Freeware

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

**HijackThis** - <http://www.spywareinfo.com/~merijn/downloads.html>

**IESPYAD** - <http://www.spywarewarrior.com/uiuc/resource.htm>

**Microsoft Defender** - <http://www.microsoft.com/athome/security/spyware/>

## Shareware

**Ad-Aware** - <http://www.lavasoft.com/>

## Some commercial anti-spyware products (not an endorsement)

**CounterSpy** - <http://www.sunbelt-software.com>

**CA Anti-Spyware** - <http://www.ca.com/us/smb/product.aspx?id=5277>

**Spy Sweeper** - <http://www.webroot.com>