

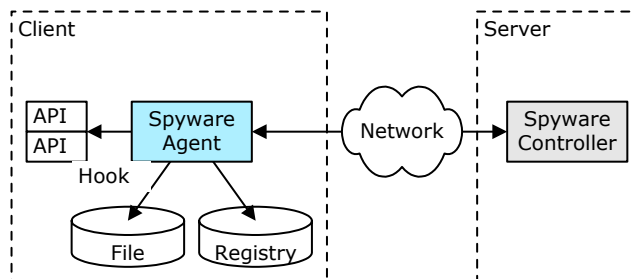
# Spyware Analysis

jan.monsch@csnc.ch

- Definition & types of spyware
- Statistics
- Hooks
- Static vs. dynamic software analysis
- Test environment for spyware
- Analysis procedure
- Spyware analysis examples
  - Dashbar/Gator
  - iGetNet
  - Windows Update
- Conclusion spyware analysis

- Spyware
  - Is a tool or mechanism that allows the spying party to do one or a combination of the following things
    - track the activities of a victim
    - steal data from a victim's system
    - modify a victim's environment
  - Often spyware requires installation of a client-side software!

- A spyware system consists of
  - client agent
    - Access to local resources, e.g. files, registry
    - Hooks itself into other applications, e.g. keyboard
  - controlling server
    - Controls the agent's behavior



- **Adware**
  - Often bundled with free software
  - Displaying pop-ups with advertisements
  
- **Adware cookies**
  - Persistent browser cookies used to uniquely identify a user for the purpose of tracking the user's surfing behavior
  - No additional software other than the browser is required

- **System monitors**
  - Capture information: Email traffic, key strokes, sites visited, screen shots, ...
  - A tool often run in the background
  - Often in combination with adware or Trojans
  
- **Trojan horses**
  - Packed with a useful application or in viruses
  - Often containing a RAT (Remote Administration Tool) giving the attacker full system access
  - Often in combination with system monitors

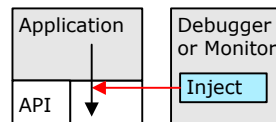
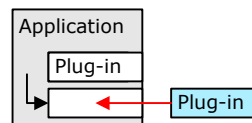
- The following show spyware-like behaviors
  - Software update
    - Application which regularly or on request check for new versions of an application
    - Often sending back license and configuration information to vendor
  - License verifier
    - Applications that contact the sever to verify the license status
    - Often found in very expensive applications

- The line between these different types of spyware is very slim. Often a tool uses a combination of them!
- Some of these spy tools are commercially available for monitoring employees, children or YOU!
- Other spyware tools are custom made for viruses or are part of as Trojan construction kits

- Recent assessment by Earthlink
  - About 1.1 Million systems have been scanned
  - About 29.5 Million spyware objects have been identified
    - System Monitors 0.2 Mio
    - Trojans 0.2 Mio
    - Adware 5.3 Mio
    - Adware Cookies 23.8 Mio

→ about 28 spyware objects per PC!!!

- A hook is a "location" in the software where additional features can be added!
  - Intentionally provided, e.g.
    - Browser Plug-ins:
      - Flash
      - Acrobat Reader, ...
    - Crypto API
      - other crypto libraries
    - Newest generation of windows anti-virus products
  - Created on purpose by the application that requests the feature, e.g.
    - Debuggers, API Monitors
    - 1<sup>st</sup> generation anti-virus products

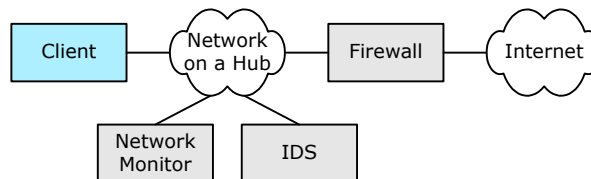


→ Hooks are very important for spyware writers as well as for spyware analysts!

- Software can be analyzed from different perspectives
  - Static
    - Snapshot based: Before and after a scenario
      - Pro: Compact overview of system changes
      - Contra: Read aspects not or minimally covered
  - Dynamic
    - Real-time based: Every application action
      - Pro: Every operation visible, including reads
      - Contra: Volume of collected material can be enormous

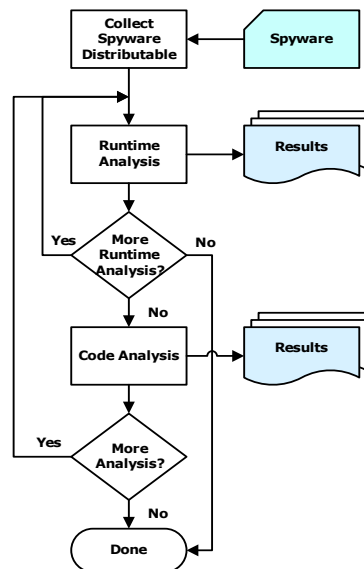
→ A good mix of both makes analysis very efficient

- Infrastructure
  - Disk image technologies for quick & easy environment setup
    - Virtual PC or VMware images (best choice)
    - Ghost or DriveImage
  - A client system totally isolated from internal network
  - Client must have network access via firewall only
  - Separate network traffic monitoring client
  - IDS when spyware is run unattended



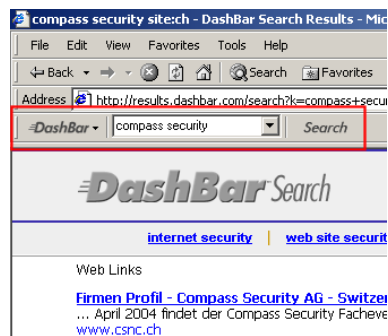
- Software required for analysis
  - Virus scanner
  - Spyware scanner
  - Personal Firewall
  - Network sniffer
  - Tool for detecting file and registry changes
  - API monitoring tools
  - Disassembler, Debugger

- Sample analysis process
- Runtime analysis
  - Execute spyware in a monitored environment
    - easy to perform
    - currently inactive code is not detected
    - stealth technologies may go undetected
- Code analysis
  - Disassemble spyware
    - every action traceable
    - time-consuming
    - Assembler skills required



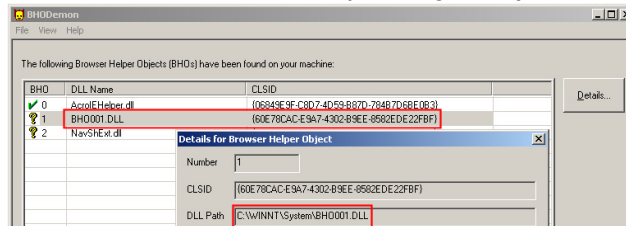
1. Isolate the spyware distributable
2. Place it on a monitored and isolated test environment
3. Create snapshots of file system and registry
4. Scan the distributable for known viruses and spyware
  - Check findings with anti-virus vendors and spyware lists
5. Run monitoring tools
  - At least: network sniffer
  - Optional: additional tools for monitoring API calls, file and/or registry access
6. Execute spyware distributable
7. Create another snapshot of file system and registry
8. Scan installation for viruses and spyware
9. Analyse the results
  - Compare the snapshots and analyse the differences
  - Analyse the output of the monitoring tools

- Dashbar is an Internet Explorer browser bar which provides access to a search engine.
- The application is rather small: ~1MB ... "cute" you think ...



- Results
  - Apart from its search-bar feature it contains a boot strap program to fetch an additional 5 MB of software components!
  - Downloads the spy and ad engine in a low priority download using byte ranges. The additional software trickles in as soon as there is an open Internet connection!
  - Used for tracking user behavior: When the user accesses a site the name's site and other information is sent to the spyware provider! As response an advertisement package is returned.
  - Uses proprietary content encryption protocols from transferring the ads and for storage on the disk.

- iGetNet uses Browser Helper Objects (a.k.a BHO)

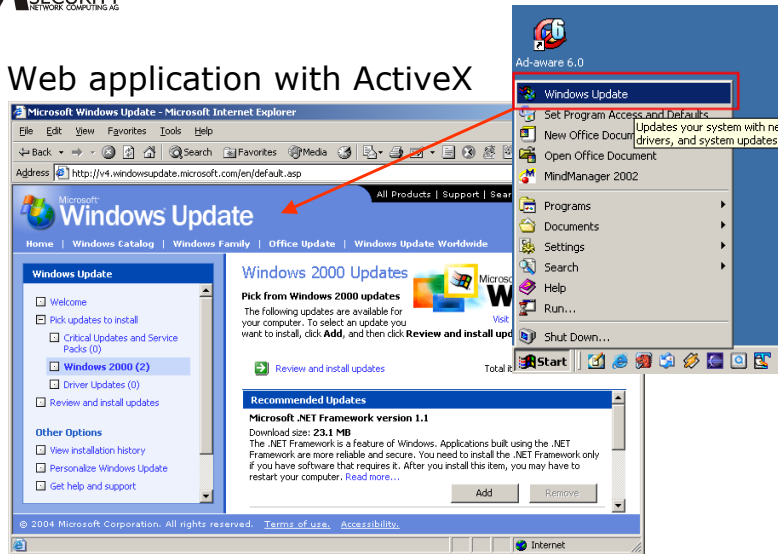


- BHO are extensions to the Internet Explorer which in one form or another are related to support surfing activities...
- Deployment often by drive-by-installation
- Often browser weaknesses are used to do unattended installations

- Results
  - Browser Helper Object (BHO)
  - Modifies the hosts file to hijack users of certain sites to the web site of the spyware provider
  - Downloads additional software from the spyware provider
  - Norton Antivirus 2004
    - does not detect the distributable as malicious when it is placed on disk or when it is installed!
    - detects it as spyware when a manual scan on the installation is performed!
    - Why? Some spywares are considered as regular commercial products!

- Introduction
  - Windows Update is a service from Microsoft to distribute application updates and security patches.
  - It is part of any Windows 2000/XP installation nowadays.
  - Since Windows 2000 SP3 Windows Update is active by default.
- How does it work?
  - Windows Update uses an ActiveX component to search the system for hardware and driver configuration.
  - This information is sent to Microsoft which in turn tells the system which patches need to be installed.

▪ Web application with ActiveX

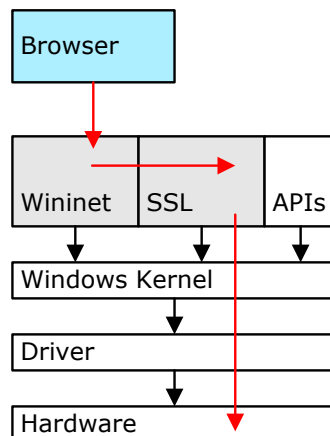


GLÄRNISCHSTRASSE 7  
POSTFACH 1671  
CH-8640 RAPPERSWIL  
Tel. +41 55-214 41 60  
Fax +41 55-214 41 61  
info@canc.ch www.canc.ch

Security Event - April 28, 2004

Page 21

- API provide services for applications and other APIs
- Several distinct APIs for different features
  - Winsock for TCP/IP
  - Crypto API
  - SSL API
  - ...

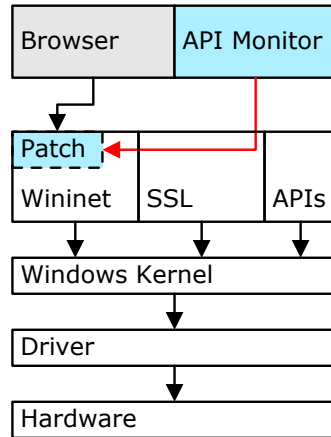


GLÄRNISCHSTRASSE 7  
POSTFACH 1671  
CH-8640 RAPPERSWIL  
Tel. +41 55-214 41 60  
Fax +41 55-214 41 61  
info@canc.ch www.canc.ch

Security Event - April 28, 2004

Page 22

- An API monitor is a debugger
- Dynamically patches APIs in their process space
- Patches intercept calls which in turn trigger the GUI



→ Read plaintext before the traffic becomes SSL

- Results
  - Users seem to be tracked

```

1047 192.168.100.88 192.168.100.88 212.254.178.165 HTTP GET http://wustat.windows.com/wutrack.bin?v=200e6638aab9cf51b4383a230b1a269e560&c=U_Site&A=1&I=win2k.windows2000.ver_p1a
1051 128.220.99.1 192.168.100.88 212.254.178.165 HTTP POST http://4.windowsupdate.microsoft.com/de/status.aspx HTTP/1.0 (apptical)
1056 128.764064 192.168.100.88 212.254.178.165 HTTP GET http://4.windowsupdate.microsoft.com/shared/js/content.js HTTP/1.0
1059 128.781817 192.168.100.88 212.254.178.165 HTTP GET http://4.windowsupdate.microsoft.com/shared/css/hcp.css HTTP/1.0
1062 128.788628 192.168.100.88 212.254.178.165 HTTP GET http://4.windowsupdate.microsoft.com/shared/css/content.css HTTP/1.0
1064 128.849431 192.168.100.88 212.254.178.165 HTTP GET http://4.windowsupdate.microsoft.com/shared/images/complete_icon.gif HTTP/1.0
    
```

- SSL encrypted connection is used to
  - Send hardware profile information to Microsoft
    - Type of Hardware used
    - Available drives and free disk space
  - Receive update and patch information
  - Fetch URLs of software download location
- The PID that techchannels found during their Windows-Update analysis does not exist any more.

- **Conclusion**
  - Antivirus products are not reliable in detecting spyware
    - Distribution package is often not recognized as malicious!
    - Spyware may go undetected until the weekly spyware scan is performed!
  - Spyware has a real chance of survival
  - Often encrypted communication protocols (SSL or proprietary) are in use for calls home to the spyware master
  - Content filters may be bypassed

- Spyware and virus information
  - SARC – Symantec Anti-Virus Research Center  
<http://www.sarc.com>
  - Spyware Guide Database  
<http://www.spywareguide.com>
  - LURHQ  
<http://www.lurhq.com>
  - List of known BHOs  
<http://www.spywareinfo.com/bhos/>
- Spyware scanners
  - Lavasoft Ad-aware  
<http://www.lavasoftusa.com>
- System snapshots
  - Winanalysis  
<http://www.winanalysis.com>

- BHO
  - BHO Daemon  
<http://www.spywareinfo.com/downloads/bhod/>
- Network sniffer
  - Ethereal  
<http://www.ethereal.com>
- API Monitors
  - Auto Debug for Windows 2.4 (commercial tool)  
<http://www.autodebug.com>
  - Sysinternals Utilities  
<http://www.sysinternals.com>
- Disassembler, Debugger
  - IDA Pro  
<http://www.datarescue.com>
  - NuMega Driver Studio  
<http://www.compuware.com>