Helping Your Users by Spying On Them

Prepared for NEbraskaCERT Conference 2005

August 11, 2005

Stephen M. Nugen, CISSP
Senior Research Fellow
Nebraska University Consortium for Information Assurance
College of IS&T, Peter Kiewit Institute
University of Nebraska, Omaha

Speaker

- Stephen (Steve) Nugen, CISSP
  - Affiliations (biases)
    - Senior Technical Research Fellow at the Nebraska University Consortium on Information Assurance, College of Information Science and Technology
    - NEbraskaCERT Board of Directors
    - Founder and President of NuGenSoft, LLC
    - Teaches: UNO, CSM, NEbraskaCERT
  - Able to monotone-mumble at useless speeds... doesn't mind when asked to slow down or repeat
  - Email welcome: smnugen@nucia.unomaha.edu;
smnugen@nugensoft.com

Overview

- With luck, presentation will be combination of lecture and demo
  - Focus is on the process as much as the results

- Flow
  - Part-1: Awareness
  - Part-2: Investigation
  - Part-3: Findings
  - Part-4: Opportunities

Part-1: Awareness

- Ref-1: Hacking Exposed: Computer Forensics
  - – Book: Hacking Exposed: Computer Forensics Secrets & Solutions, 2005
    - Relatively recent publication
  - – Page 136
    - "When a user executes a program or accesses certain types of files in Windows XP, a built-in Windows function documents his or her actions."
    - "User Assist is a new feature in Windows XP that is not well documented or well understood by the public."
    - "It is like a built-in spyware tool that cannot be disabled..."

Part-1: Awareness cont'd

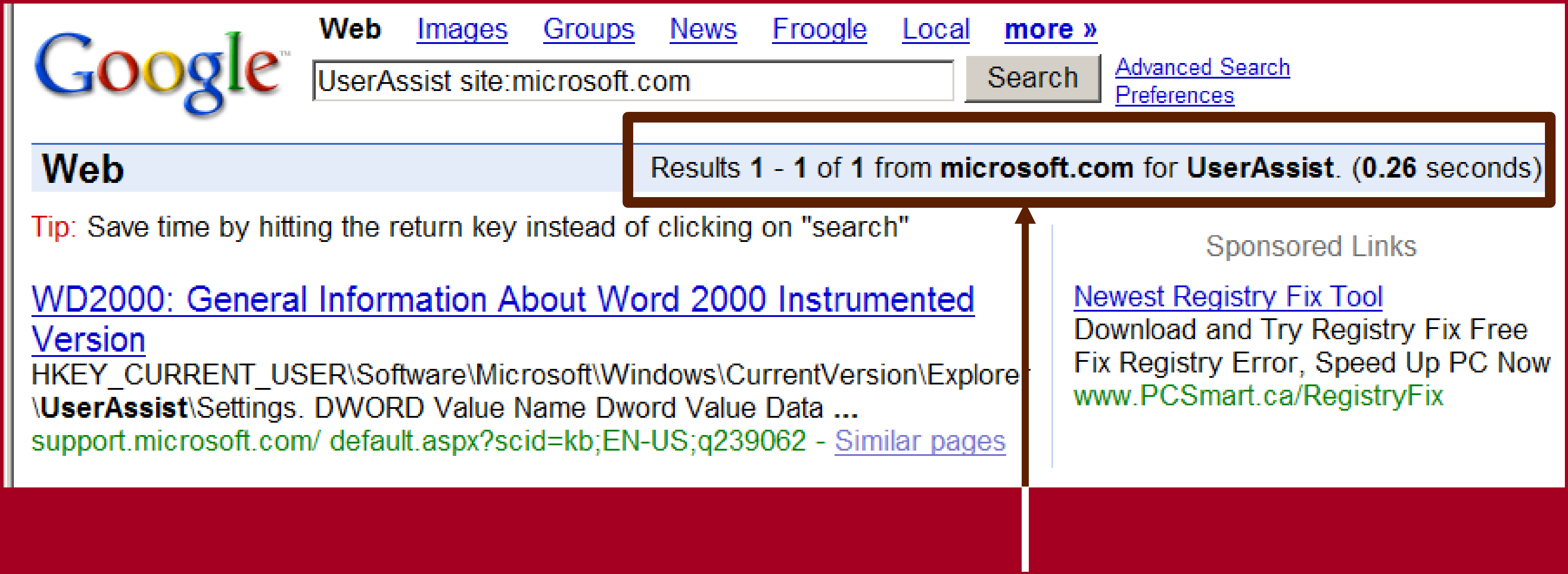
- Ref-1, page 136 cont'd
  - "It captures the actions of a user until someone or something removes the entries from the registry."
  - "User Assist entries are encrypted, but... they are encrypted with ROT 13!"
  - User Assist entries stored in registry:
    HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist

Part-1: Awareness cont'd

- This is enough to motivate some checks...
  - Demo-1
    - Target: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist...
    - Tool: Regedit
  - Demo-2
    - Target: Encrypted entries
    - Tool: MS Excel
  - Demo-3
    - Target: Effect of cleaning IE and Explorer caches
    - Tools: IE, Taskbar, Regedit

Part-2: Investigation

- What does Microsoft.com say about this?
  - Google search: UserAssist site:microsoft.com
    - Just search for results within microsoft.com



UserAssist site:microsoft.com

Results **1** - **1** of **1** from **microsoft.com** for **UserAssist**. (**0.26** seconds)

Tip: Save time by hitting the return key instead of clicking on "search"

WD2000: General Information About Word 2000 Instrumented Version
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\Settings. DWORD Value Name Dword Value Data ...
support.microsoft.com/ default.aspx?scid=kb;EN-US;q239062 - Similar pages

Newest Registry Fix Tool
Download and Try Registry Fix Free
Fix Registry Error, Speed Up PC Now
www.PCSmart.ca/RegistryFix

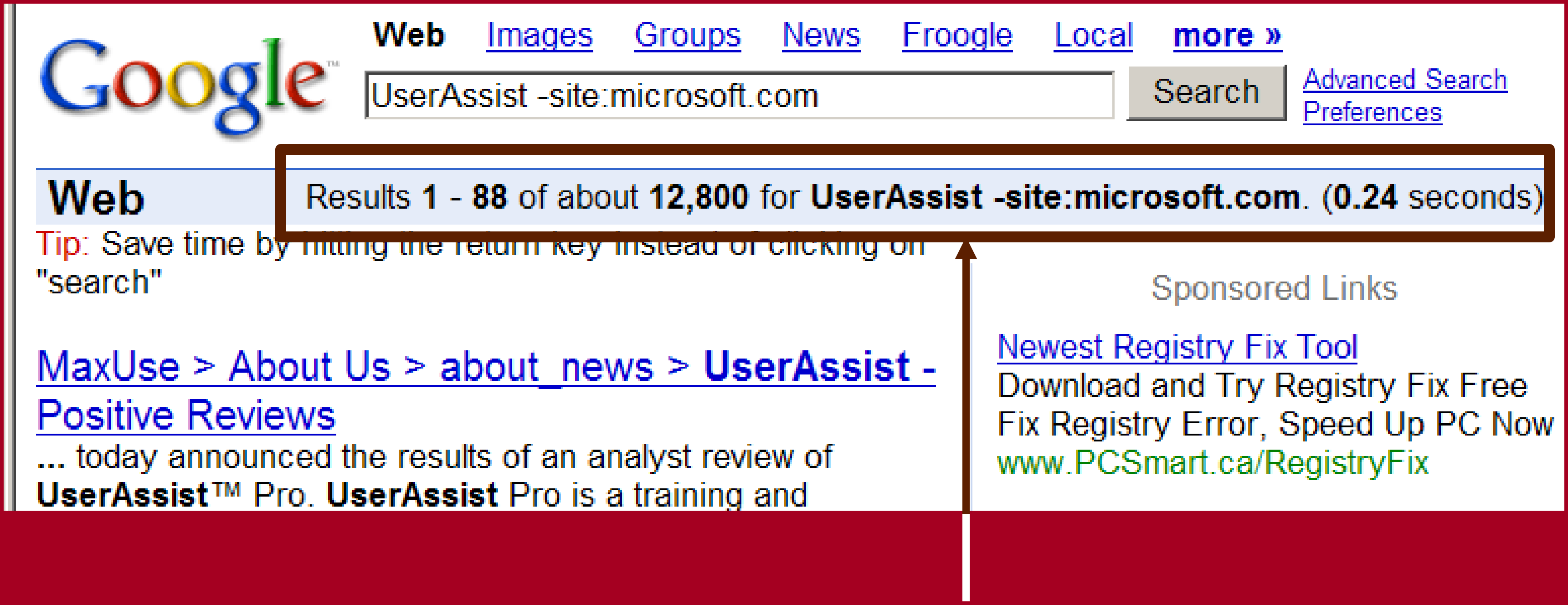
One result... for special version of MS Word 2000

Part-2: Investigation cont'd

- What does Microsoft say cont'd
  - MS Word 2000 Instrumented Version
    - Research program that helps Microsoft gather information about how certain functions in Word and Office are used
    - Information stored as files with *.rsh extensions
    - Created registry entries include:
      - HKEY_CURRENT_USER\Software\Microsoft \Windows\CurrentVersion\Explorer \UserAssist\Settings
  - Not exactly on-target since
    - Different registry keys... no files with .rsh extensions
    - <Check to be sure>

Part-2: Investigation cont'd

- What about non-MS sources?
  - Google search: UserAssist -site:microsoft.com
    - Any domain other than microsoft.com



UserAssist -site:microsoft.com

Web Results **1** - **88** of about **12,800** for **UserAssist -site:microsoft.com**. (**0.24** seconds)

Tip: Save time by hitting the return key instead of clicking on "search"

MaxUse > About Us > about_news > **UserAssist** - Positive Reviews

... today announced the results of an analyst review of **UserAssist**™ Pro. **UserAssist** Pro is a training and

Sponsored Links

Newest Registry Fix Tool

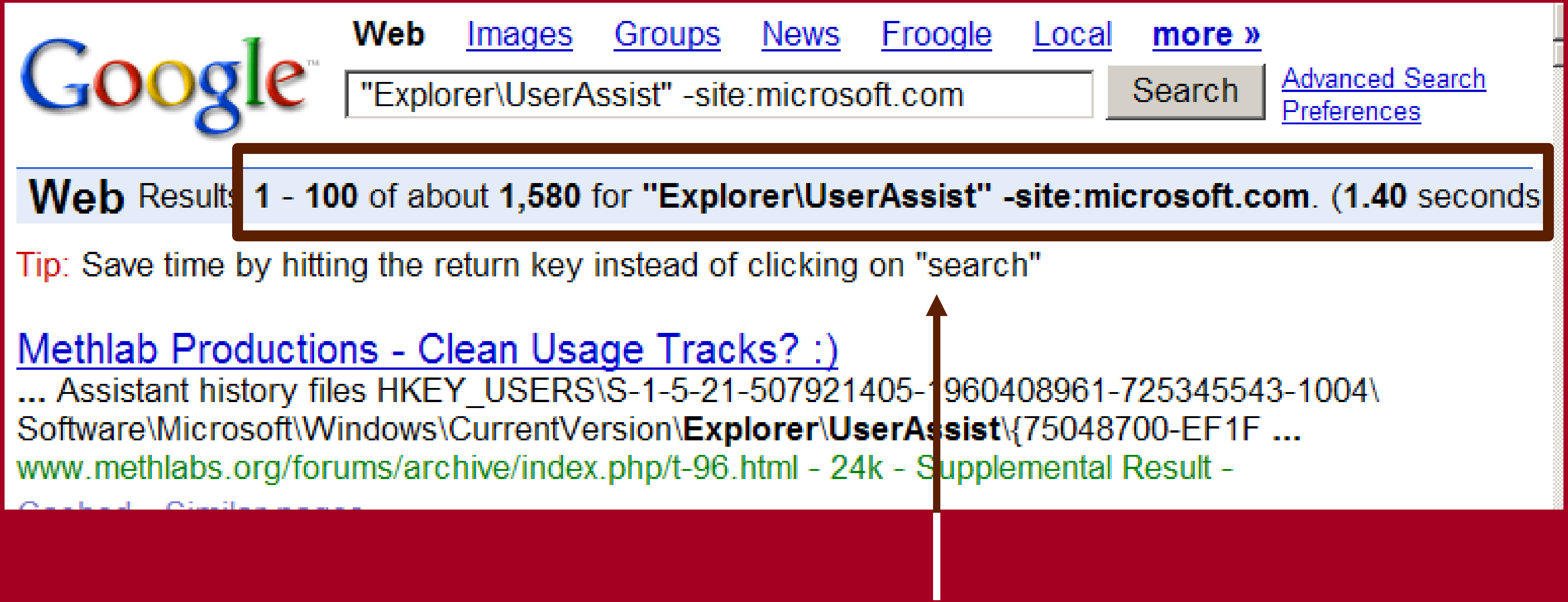
Download and Try Registry Fix Free Fix Registry Error, Speed Up PC Now

www.PCSmart.ca/RegistryFix

12,800 Results... way, way more than I hoped for

Part-2: Investigation cont'd

- Non-MS sources cont'd
  - More restricted Google search: Explorer\UserAssist -site:microsoft.com



"Explorer\UserAssist" -site:microsoft.com

Web Results **1** - **100** of about **1,580** for **"Explorer\UserAssist" -site:microsoft.com**. (**1.40** seconds

Tip: Save time by hitting the return key instead of clicking on "search"

Methlab Productions - Clean Usage Tracks? :)
... Assistant history files HKEY_USERS\S-1-5-21-507921405-1960408961-725345543-1004\ Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F ...
www.methlabs.org/forums/archive/index.php/t-96.html - 24k - Supplemental Result -

1,580 Results... getting closer

Part-2: Investigation cont'd

- Ref-2: explorer_spy.txt (updated)
  - Meta
    - Title: Yet Another Method Windows Uses to Log Your Computer Activity
    - Author: Jeremy Bryan Smith aka Helamonster
    - Source for updated (2003-08-18) version: http://www.utdallas.edu/~jbs024000/articles/explorer_spy.html
    - Excerpts reformatted and reworded for brevity

Part-2: Investigation cont'd

- Ref-2 cont'd
  - Poking around registry found these suspicious keys:
    - HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{5E6AB780-7743-11CF-A12B-00AA004AE837}\Count
    - HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count
  - Entries encrypted with ROT-13
  - Decrypted entries refer to URLs, programs, and so forth

Part-2: Investigation cont'd

- Ref-2 cont'd
  - Both count keys had entries corresponding to
    - Files not accessed since Windows first installed
    - Files and URLs not accessed for years
  - Information always collected, never deleted
    - One key had 18,497 entries
    - Other key had 394 entries
    - Over time, contributes to
      - Registry bloat
      - Registry fragmentation
      - Windows slow down

Part-2: Investigation cont'd

- Ref-2 cont'd
  - First hypothesis: Computer infected with ***Malware***
    - Program updating these keys: EXPLORER.EXE
    - Unmodified from Windows 2000 SP1 distribution
  - Second hypothesis: What looks like malware is actually an undocumented ***feature*** in MS Windows
  - Third hypothesis: You can make Windows faster and more respectful of your privacy if you simply "delete those dumb keys at every logon/logoff"

Part-2: Investigation cont'd

- Ref-3: Vic Ferri, WinTips and Tricks
  - Meta
    - Title: The Count Keys in the Windows Registry: What They Do, How To Understand Them, and How To Remove Them
    - Author: Vic Ferri, WinTips and Tricks
    - Source: http://personal-computer-tutor.com/abc3/v29/vic29.htm
    - Excerpts reformatted and reworded for brevity

Part-2: Investigation cont'd

- Ref-3 cont'd
  - Count keys lesser known, rather mysterious registry keys
  - Used to log some online and offline activities
  - Leads one to believe that these are "spyware" keys but:
    - These keys are also used by legitimate sources - both online and offline
    - Online, many sites you consider trustworthy may add info to these keys when you visit them
      - Example: Google creates/updates entries when you visit their site(s)

Part-2: Investigation cont'd

- Ref-3 cont'd
  - Choice: Delete these keys... recreated at next login
  - Choice: Stop the logging
    - Not documented or supported by Microsoft, so
      - Your mileage may vary
      - May leave system in unusable state (right away or after next Windows Update)
    - Method
      - Add a new key to UserAssist: 'Settings'
      - Add new value to 'Settings': DWORD NoLog 1
Reboot (and pray)

Part-2: Investigation cont'd

- Ref-3 cont'd
  - Choice: Stop the encryption
    - Not documented or supported by Microsoft, so
      - Your mileage may vary
      - May leave system in unusable state (right away; or after next Windows Update; or after next full moon)
    - Method
      - Add a new key to UserAssist: 'Settings'
      - Add new value to 'Settings': DWORD NoEncrypt 1
      - Reboot; Pray it works
      - Old entries still encrypted, but new entries should be unencrypted

Part-2: Investigation cont'd

- How to determine which user events recorded in these keys
  - Option-1
    - View registry with regedit
    - Perform event
    - View registry with regedit, look for changes
    - Real ugly

Part-2: Investigation cont'd

- How to determine cont'd
  - Option-2
    - Export registry tree with regedit
    - Perform event(s)
    - Export registry tree
    - Compare
    - Still ugly
  - Option-3
    - Use (free) regmon tool to detect changes in real-time
      - Source: www.sysinternals.com

Part-2: Investigation cont'd

- Determine which events recorded
  - Demo-4
    - Target: Registry changes
    - Tool: Regmon, no filters
  - Demo-5
    - Target: Selected registry changes
    - Tool: Regmon with filters
  - Demo-6
    - Target: Decrypt registry changes
    - Tools
      - Regmon, filtered, exported logs
      - Excel to decrypt line by line

Part-2: Investigation cont'd

- Determine which events recorded cont'd
  - Demo-7
    - Target: Viewing impact of series of events
    - Tools:
      - Regmon, filtered, exported logs
      - Excel to trim
      - VBS Script to decrypt sequence
  - Demo-8
    - Target: Viewing impact of series of events
    - Tools:
      - Regedit to delete; add NoEncrypt; Reboot
      - Regmon, filtered, view

Part-2: Investigation cont'd

- Determine which events recorded cont'd
  - Demo-9
    - Target: Same as Demo-8, focusing on events, not methods
      - Windows explorer: buttons; document shortcuts; program shortcuts
      - Internet explorer: favorites (name vs url); new favorites; typed urls; etc.
      - Firefox
      - Command line
      - Etc.

Part-3: Findings

- Is this spyware?
  - Depends on your point of view
    - Ref: Spyware definitions from Bill Hayes' presentation
  - Yes
    - Information about user activities is collected without their knowledge or consent
    - Collected information includes <selected> web site behavior
    - Part of a for-profit product managed by a business venture
    - Collected information is probably intended for market research, but it can also be used for industrial or national espionage

Part-3: Findings

- Is this spyware cont'd
  - No
    - No reports of this collected information being sent to an outside source without users' knowledge
    - No reports of this collected information containing user PII information considered real private (e.g., authentication credentials, SSN, etc.)
    - Doesn't change how the computer interacts with the user
      - Unless it slows down... presumably unintentional

Part-3: Findings

- Is this spyware cont'd
  - Depends... What if Microsoft
    - Discontinued collecting information related to web sites?
    - Changed to stronger encryption?
    - Sent information about how you use your computer and network to Microsoft servers:
      - To help them design future operating systems, better suited to your activities?
        - » *Consistent with description for MS Word 2000 IV*
      - For resale to other organizations?
        - » Example: A user with extensive bookmarks related to cruises would probably be a high-value "mark" for cruise lines seeking potential customers

Part-3: Findings

- Are web sites like google updating local registry?
- Is the monitoring comprehensive?
- Is this new, or exclusive to, Windows XP?

Part-4: Opportunities

- Augment the capabilities of your favorite applications and/or operating systems
  - Extend the concept of personalized menus to include buttons, IE favorites, desktop items, etc..
  - Collect the information from multiple clients into a single DB for study, future improvements
- Augment the capabilities of your favorite spyware package
  - Collect information for sharper user profiles, resale

Part-4: Opportunities cont'd

- Use in an enterprise, with remote registry service, to monitor your employees
  - Detect and record off-task activities
  - No need to install obnoxious client-side software... can do it all server-side

Note: This concept could be extended to remote monitoring of virtual enterprises where member clients unwittingly self-nominate themselves by connecting to the network with insufficient safeguards

Part-4: Opportunities cont'd

- Protect yourself, your organization from unauthorized collection, disclosure
  - Delete the keys
    - Every logoff
    - After especially interesting series of events
  - Disable logging via 'NoInstrumentation' described in multiple ***Microsoft*** KB articles, including 292504
    - With Group Policy Editor (strongly preferred)
      - User Configuration \ Administrative Templates \ Start Menu and Taskbar

Part-4: Opportunities cont'd

- Protecting yourself cont'd
  - Disable logging via 'NoInstrumentation' cont'd
    - With regedit
      - Key: 'HKCU\Software\Microsoft\Windows \CurrentVersion\Policies\Explorer
      - NoInstrumentation DWORD
        - » 0 (or missing): Enable user tracking
        - » 1: Disable user tracking... disables customized menus, etc.
  - Disable logging via 'NoLog' described by Ref-3
    - Risk unknown

Finished

- Summary
  - First reports very helpful, but not always complete
  - Simple free tools can be used to determine what's happening
  - UserAssist entries have the potential to support multiple opportunities, some of which you may want to prevent
- Questions?