CERIAS

the center for education and research in information assurance and security

Yahoo Messenger Forensics

for Windows Vista and Windows 7

Matt Levendoski, Tejashree Datar, Marc Rogers, Det. Paul Huff

Abstract

The purpose of this study is to indicate several areas of interest within the Yahoo! Messenger application that are of forensic significance. This study will mainly focus on new areas of interest within the file structure of Windows Vista and Windows 7. One of the main issues with this topic is that little research has been previously conducted on the new Windows platforms. The previously conducted research indicates evidence found on older file structures, such as Windows XP, as well as outdated versions of Yahoo! Messenger.

Gap Analysis

Newer versions of this software have been released and new capabilities within the technology have introduced new areas of evidence. The trends have shifted with the introduction and use of Windows Vista and Windows 7. We are seeing more computers running these updated platforms nullifying some of the articles previously found on Windows XP. The review of previous articles have helped create a basis of the core elements of the software as well as allow for the discovery of future artifacts.

Methodology

- VMWare Fusion running on Mac Pro Environment
- 2 virtual machines (Windows Vista & Windows 7)
- Latest version of Yahoo Messenger (10.0.0.1258)
- 3 test accounts (2 Predators & 1 victim)
- Initiated chats, file transfers, photo sharing between accounts
- Interactions tracked and logged via Virtual Snapshots

File Transfer

There are two ways of sharing photos. One is via Yahoo Photo Sharing and the other is via the file transfer option. If the user wishes to save the photos shared via Photo Sharing, the default save folder is in the 'Picture' folder.

File transfer option can be used to transfer all kind of files such as photos, documents, music. Default location while saving a file during file transfer is Documents. But, if the user wishes to, the file can be saved anywhere on the computer. The default file name is the same as the original file. The date-time stamp of the saved file is that of the local machine at the date/time the file was saved.

Yahoo! Registry at a Glance

File	Location	Description	Windows Vista	Windows 7
HKEY_CURRENT_USER	\Software\Yahoo\Pager	Gives the Yahoo ID of the user	Yahoo user id	Yahoo user id
		Gives the installed version of Yahoo Messenger	Yahoo version	Yahoo version
		Gives the version revisions of Yahoo Messenger	Yahoo version revisions	Yahoo version revisions
		Shows if the password is saved	Saved password	Saved password
		Shows if auto sign in for Yahoo Messenger is turned on or off	Auto sign in	Auto sign in
		Shows the number of allowed P2P users	P2P count	
HKEY_CURRENT_USER	\Software\Yahoo\Pager\profiles\profile_name\chat	Gives the last selected chat room category	Chat	Chat
HKEY_CURRENT_USER	\Software\Yahoo\Pager\profiles\profile_name\chat\favorite rooms	Gives the list of saved favorite rooms for the user	Favorite Room	Favorite Room
HKEY_CURRENT_USER	\Software\Yahoo\Pager\profiles\profile_name\FT	gives the last saved location of a received file and the last sent location of a transferred file	FT	FT
HKEY_CURRENT_USER	Software\Yahoo\Pager\profiles\profile_name\FriendIcons	Gives the icon that the user has set for himself/herself that is displayed to the user's friends.	FriendIcons	FriendIcons

Photo Sharing

Whenever a photo sharing session is initiated, a photo sharing folder starting with the letter 'S' and randomly assigned numbers and letters is created in the Program Data folder. The path for the created 'S' folder is as follows: 'C:\ProgramData\Yahoo!\Messenger\PhotoSharing\Sc8b0'. Once the session is initiated, as soon as the other yahoo user accepts the photo sharing invite, the 'S' folder is created in the PhotoSharing folder on the initiator's side. The 'S' folder in itself is empty until any pictures are shared. As soon as an image is shared (sent), a thumbs file '_t.jpg' is created followed by the image file '_m.jpg'.

Selected References

AccessData. (2005). Registry Quick Find Chart.

Dickson, M. (2006). An examination into Yahoo Messenger 7.0 contact identification [Electronic Version]. *Digital Investigation, 3,* 159 – 165.

Wagner, Lt. (Ret) Steven. (February, 2007). PhotoSharing Folder – Yahoo Messenger. *Source – Encase message boards*. 1 – 1.

Unknown. (n.d.). Yahoo! Messenger Photo Sharing. 1 - 13

PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center