Analysis Report

FOR A893.EXE

[Contains a brief malware analysis report for the file sample.exe which was provides as an assignment during the SecurityXploded Student Mentorship Programme]

Mentor: Amit Malik and Monnappa KA

By Sajan Shetty

Tel : +919964224668
Email : me@thewiredgoon.com
ixcodxdx@gmail.com

Website : www.TheWiredGoon.com
Twitter: TheWiredGoon

Contents

"Zeus is a Trojan horse that steals banking information by Man-in-the-browser keystroke logging and Form Grabbing."

Introduction and Technical Analysis

General Information

- File Name : a893.exe
- MD5 : a893bbf7c1d45bc0532e7b336a442e22
- SHA-1 : 10958a2010f731035ae6575d3e7ed75d00b6ca8d
- Detected as : TROJ_GEN.RCBC7HH
- Other know Aliases : TrojanSpy.Zbot.epqg, Trojan.Win32.A.Zbot.198145.AT, TrojanPWS.Zbot.Y

Analysis Overview

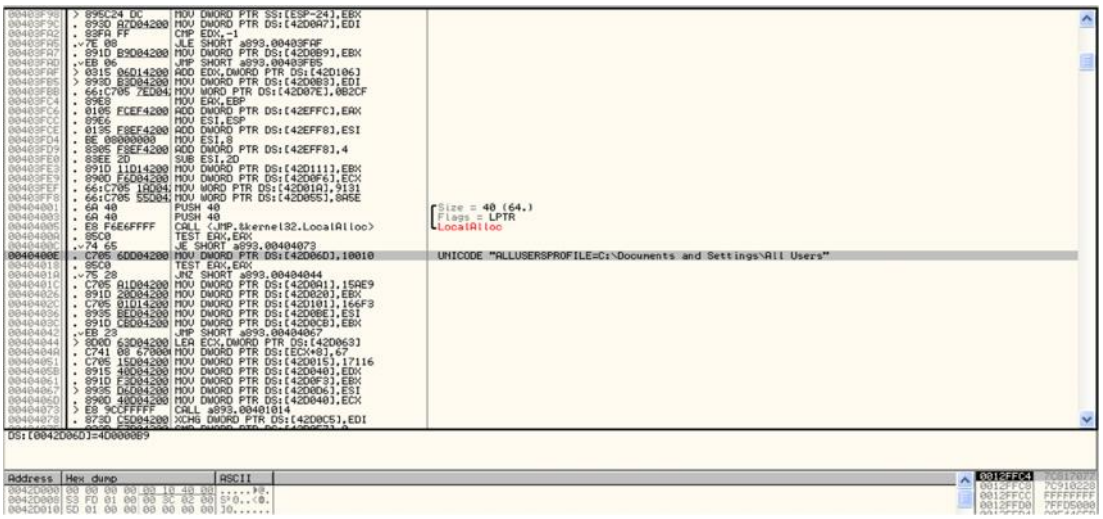
a893.exe is a generic detection for a password stealer and remote access trojan.

Technical Analysis

- The file spawns new process.
- It copies a new malicious exe file to *<drive:>\documents and settings\<user name>\application data*
- The md5 hash sum of the new malicious exe file at *<drive:>\documents and settings\<user name>\application data* is completely different from our initial sample file.
- The file name and the folder name generated at is *<drive:>\documents and settings\<user name>\application data* randomized.
- It creates and modifies registry entries.
- The registry entry is modified to the run the dropped malware at Windows start.
- It tampers with execution of other processes.
- The malware can inject code into user level programs like explorer.exe
- It changes the setting of Internet Explorer.

Introduction and Technical Analysis

- It hooks with Windows API's to perform various malicious operations and capture sensitive data.



Above is the code excerpt from the Trojan.

System Activity

Registry changes

This malware creates the following registry entries add adds the folder name and the file created by it at *<drive:>\documents and settings\<user name>\application data*

HKU\S-1-5-21-842925246-1425521274-308236825-500\SOFTWARE\Microsoft\Niiw

It also creates new registry keys for Internet Explorer

The following registry entries are Read
HKLM\System\CurrentControlSet\Control\Terminal Server HKLM\System\CurrentControlSet\
HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5

File Changes

It creates a new file and folders at *<drive:>\documents and settings\<user name>\application data*

C:\Documents and Settings\Administrator\Application Data\Epteaz

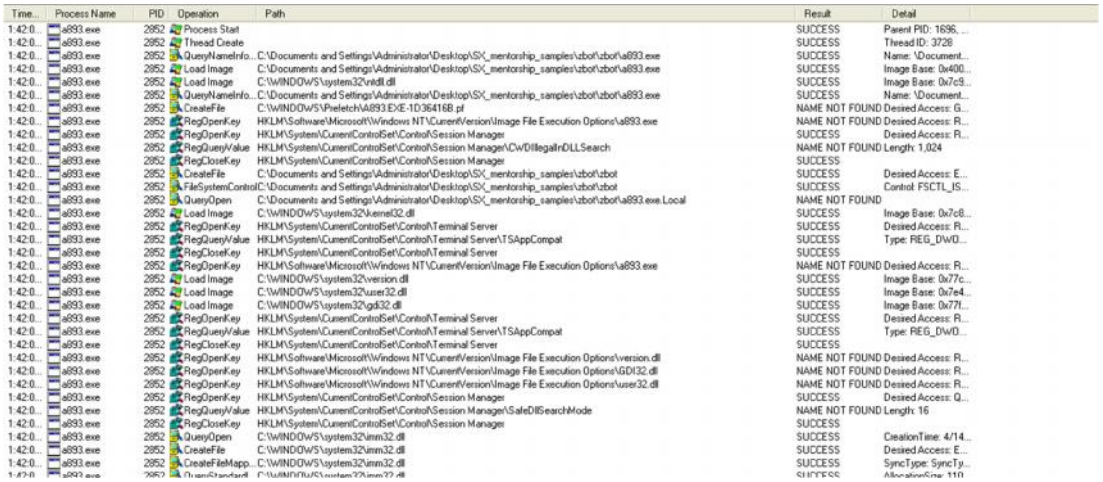
C:\Documents and Settings\Administrator\Application Data\Epteaz\umbal.ynz

C:\Documents and Settings\Administrator\Application Data\Niif

C:\Documents and Settings\Administrator\Application Data\Niif\docuu.exe

The file also inject into user level process like explorer.exe

System Activity



Time...	Process Name	PID	Operation	Path	Result	Detail
1:42:0...	a893.exe	2952	Process Start		SUCCESS	Parent PID: 1696, ...
1:42:0...	a893.exe	2952	Thread Create		SUCCESS	Thread ID: 3728
1:42:0...	a893.exe	2952	QueryNameInfo...	C:\Documents and Settings\Administrator\Desktop\SX(_mentorship_samples\zbot\zbot\a893.exe	SUCCESS	Name: \Document...
1:42:0...	a893.exe	2952	Load Image	C:\Documents and Settings\Administrator\Desktop\SX(_mentorship_samples\zbot\zbot\a893.exe	SUCCESS	Image Base: 0x400...
1:42:0...	a893.exe	2952	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Image Base: 0x7c9...
1:42:0...	a893.exe	2952	QueryNameInfo...	C:\Documents and Settings\Administrator\Desktop\SX(_mentorship_samples\zbot\zbot\a893.exe	SUCCESS	Name: \Document...
1:42:0...	a893.exe	2952	CreateFile	C:\WINDOWS\Prefetch\A893.EXE-1D36416B.pf	NAME NOT FOUND	Desired Access: G...
1:42:0...	a893.exe	2952	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\a893.exe	NAME NOT FOUND	Desired Access: R...
1:42:0...	a893.exe	2952	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: R...
1:42:0...	a893.exe	2952	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\CWDIllegalInDLLSearch	NAME NOT FOUND	Length: 1,024
1:42:0...	a893.exe	2952	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	
1:42:0...	a893.exe	2952	CreateFile	C:\Documents and Settings\Administrator\Desktop\SX(_mentorship_samples\zbot\zbot	SUCCESS	Desired Access: E...
1:42:0...	a893.exe	2952	FileSystemControl	C:\Documents and Settings\Administrator\Desktop\SX(_mentorship_samples\zbot\zbot	SUCCESS	Control: FSCTL_IS...
1:42:0...	a893.exe	2952	QueryOpen	C:\Documents and Settings\Administrator\Desktop\SX(_mentorship_samples\zbot\zbot\a893.exe.Local	NAME NOT FOUND	
1:42:0...	a893.exe	2952	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 0x7c8...
1:42:0...	a893.exe	2952	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	Desired Access: R...
1:42:0...	a893.exe	2952	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat	SUCCESS	Type: REG_DWO...
1:42:0...	a893.exe	2952	RegCloseKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	
1:42:0...	a893.exe	2952	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\a893.exe	NAME NOT FOUND	Desired Access: R...
1:42:0...	a893.exe	2952	Load Image	C:\WINDOWS\system32\version.dll	SUCCESS	Image Base: 0x77c...
1:42:0...	a893.exe	2952	Load Image	C:\WINDOWS\system32\user32.dll	SUCCESS	Image Base: 0x7e4...
1:42:0...	a893.exe	2952	Load Image	C:\WINDOWS\system32\gdi32.dll	SUCCESS	Image Base: 0x77f...
1:42:0...	a893.exe	2952	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	Desired Access: R...
1:42:0...	a893.exe	2952	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat	SUCCESS	Type: REG_DWO...
1:42:0...	a893.exe	2952	RegCloseKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	
1:42:0...	a893.exe	2952	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\version.dll	NAME NOT FOUND	Desired Access: R...
1:42:0...	a893.exe	2952	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\GDI32.dll	NAME NOT FOUND	Desired Access: R...
1:42:0...	a893.exe	2952	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\user32.dll	NAME NOT FOUND	Desired Access: R...
1:42:0...	a893.exe	2952	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Q...
1:42:0...	a893.exe	2952	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\SafeDllSearchMode	NAME NOT FOUND	Length: 16
1:42:0...	a893.exe	2952	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	
1:42:0...	a893.exe	2952	QueryOpen	C:\WINDOWS\system32\imm32.dll	SUCCESS	CreationTime: 4/14...
1:42:0...	a893.exe	2952	CreateFile	C:\WINDOWS\system32\imm32.dll	SUCCESS	Desired Access: E...
1:42:0...	a893.exe	2952	CreateFileMapp...	C:\WINDOWS\system32\imm32.dll	SUCCESS	SyncType: SyncTy...

An Image excerpt from Process monitor showing all file and registry operations