

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

Introduction and Technical Analysis	1
General Information	1
Analysis Overview	1
Technical Analysis	1
System Activity	3
Registry changes	3
File Changes	3

“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.

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

```

00403F98 > 89C24 DC MOV DWORD PTR DS:[ESP-24],EBX
00403F9C • 8930 A7D04200 MOV DWORD PTR DS:[42D0A7],EDI
00403F9E • 8F91 FE CMP EDI,-1
00403FA2 • 7E 08 JLE SHORT 8930,00403FAE
00403FA7 • 89D84200 MOV DWORD PTR DS:[42D089],EBX
00403FAD • EB 05 JMP SHORT 8930,00403FEE
00403FAF > 0315 06D14200 ADD EDI,DWORD PTR DS:[42D106]
00403FB5 > 89D84200 MOV DWORD PTR DS:[42D089],EDI
00403FB8 • 66C705 7ED04 MOV WORD PTR DS:[42D07E],0B2CF
00403FC4 • 89E5 MOV EAX,EBP
00403FC6 • 0195 ECE4200 ADD DWORD PTR DS:[42EFC],EAX
00403FCC • 89E6 MOV ESI,ESP
00403FCE • 0195 F8E4200 ADD DWORD PTR DS:[42EFF8],ESI
00403FD4 • BE 00000000 MOV ESI,0
00403FD7 • 89E5 F8E4200 ADD DWORD PTR DS:[42EFF8],4
00403FE0 • 89EE 20 SUB ESI,20
00403FE3 • 891D 11D14200 MOV DWORD PTR DS:[42D111],EBX
00403FE7 • 89D0 F084200 MOV DWORD PTR DS:[42D0F3],ECX
00403FEF • 66C705 10D04 MOV WORD PTR DS:[42D010],9131
00403FF6 • 66C705 55D04 MOV WORD PTR DS:[42D055],845E
00404001 • 6A 40 PUSH 40
00404003 • 6A 40 PUSH 40
00404005 • E5 F8E4FFFF CALL JMP,Kernel32.LocalAlloc>
0040400A • 85C0 TEST EAX,EAX
0040400C • 74 65 JZ SHORT 8930,00404073
0040400E • C705 60D04200 MOV DWORD PTR DS:[42D06D],10010
00404010 • 85C0 TEST EAX,EAX
00404012 • 75 28 JNZ SHORT 8930,00404044
0040401C • C705 A1D04200 MOV DWORD PTR DS:[42D0A1],15AE9
00404020 • 891D 28D04200 MOV DWORD PTR DS:[42D020],EBX
00404026 • C705 01D14200 MOV DWORD PTR DS:[42D101],166F3
00404036 • 8935 EDD04200 MOV DWORD PTR DS:[42D0BE],ESI
0040403C • 891D CDD04200 MOV DWORD PTR DS:[42D0C0],EBX
00404042 • EB 23 JMP SHORT 8930,00404067
00404044 > 89D0 60D04200 LEA ECX,DWORD PTR DS:[42D063]
00404048 • C741 08 67D04 MOV DWORD PTR DS:[ECX+8],67
00404051 • C705 15D04200 MOV DWORD PTR DS:[42D015],17116
0040405B • 8915 4DD04200 MOV DWORD PTR DS:[42D04D],EBX
00404061 • 891D F3D04200 MOV DWORD PTR DS:[42D0F3],EBX
00404067 • 8935 DDD04200 MOV DWORD PTR DS:[42D063],ESI
0040406D • 89D0 4DD04200 MOV DWORD PTR DS:[42D04D],ECX
00404073 > E9 9CFFFFFF CALL 8930,00401014
00404078 • 89D0 CDD04200 MOV DWORD PTR DS:[42D0C0],EDI
0040407E • 89E5 07D04200 MOV DWORD PTR DS:[42D053],EAX
DS:[0042D06D]=40000009

```

Address	Hex dump	ASCII
0042D090	00 00 00 00 00 00 10 00 00P.
0042D098	53 F0 01 00 00 00 00 00 00	S@...@.
0042D0A0	50 01 00 00 00 00 00 00 00	0.....

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

