

Analysis Report

FOR SAMPLE1.EXE

[Contains a brief malware analysis report for the file sample.exe which was provided 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
Network Activity.....	4

“A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers.”

Introduction and Technical Analysis

General Information

- File Name : Sample1.exe
- MD5 : ae8a0e6cac52929cc48e1b7074eba86c
- SHA-1 : 84705f524f4949234692f50263ac19bbbe97f281
- Detected as : WORM_SPYBOT.CCF
- Other know Aliases : W32.Randex.gen, W32/Sdbot-Fam, Backdoor.Win32.IRCBot.gen, TR/Crypt.ULPM.Gen,W32/Sdbot.worm.gen

Analysis Overview

Sample1.exe was identified as ‘WORM_SPYBOT.CCF’ which is a computer worm that connects to a host server IP and takes instructions from the attacker. This worm has a backdoor component helping attacker to gain full system access and to spread to other computers in the network

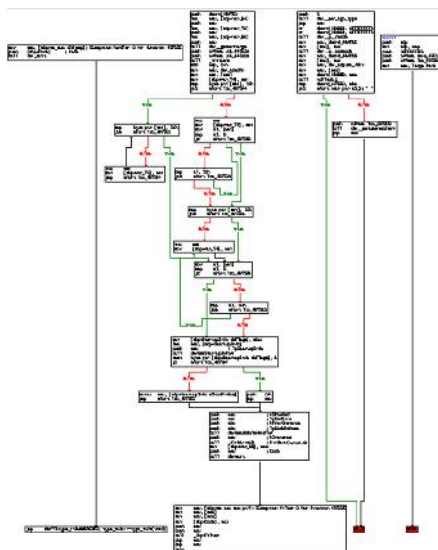
Technical Analysis

- The worm copies itself as services32.exe in system32 directory.
- It modifies and Adds new registry keys to victim machine so that it runs every time Windows starts.
- It exploits a buffer overrun vulnerability in Windows Service named ‘LSASS’.
- The attacker has full system privileges and can perform remote code execution.
- It connects to a remote IP address (217.22.59.29) to receive commands from the attacker.
- It can also run and manipulate files as specified by the attacker.
- It steals Windows Product Keys.
- It also steals game keys of popular games like Call of Duty, Soldier of fortune etc.
- It also steals credentials of Yahoo and AOL Messengers.
- It can conduct a Denial of Service attack.

- Create an HTTP or FTP server on the victim machine.
- Spread to other vulnerable computers by exploiting vulnerabilities

```
.data:0044528 align 10h
.data:0044530 aScanCouldnTSto db 'scan: couldn',27h,'t stop',0 ; DATA XREF: sub_422D50+10Afo
.data:0044544 align 8
.data:0044548 aScanStopped0Th db 'scan: stopped (%d threads)',0
.data:0044548 ; DATA XREF: sub_422D50+197fo
.data:0044563 align 8
.data:0044568 aFtpPortDTotalS db 'ftp: port: %d, total sends: %d',0
.data:0044568 ; DATA XREF: sub_422D50+140fo
.data:0044587 align 10h
.data:0044590 aScanNotStarted db 'scan: not started',0 ; DATA XREF: sub_422D50+B2fo
.data:00445A2 align 8
.data:00445A8 aScanCipS db 'scan: cip (%s)',0 ; DATA XREF: sub_422D50+6Dfo
.data:00445B7 db 0
.data:00445B8 db 0
.data:00445B9 db 0
.data:00445BA db 0
.data:00445BB db 0
.data:00445BC aSExploitedS db '%s: exploited (%s)',0 ; DATA XREF: sub_423900+2Cfo
.data:00445CF db 0
.data:00445D0 db 0
.data:00445D1 db 0
.data:00445D2 db 0
.data:00445D3 db 0
.data:00445D4 aSocketClosed_ db 'Socket closed.',0 ; DATA XREF: .text:loc_423E93fo
```

Above is the code excerpt from the worm which exploits 'LSASS' Windows Service



Above is the graph of execution flow of the worm

Network Activity

The Worm tries to connect to remote IP address (217.22.59.29) from where the attacker sends commands to be performed on the victim machine. It uses the port no 6667 to talk to the attacker.

The worm opened up a tcp port, with no 5307 to listen to the attacker server.

An image from Wireshark showing the IP address the worm is trying to connect to

14	18.952687	192.168.75.134	217.22.59.29	TCP	62	31-11	>	6667	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM=1	
15	18.953014	217.22.59.29	192.168.75.134	TCP	60	6667	>	31-11	[RST, ACK]	Seq=3871684576	Ack=1	Win=64240	Len=0		
16	19.390067	192.168.75.134	217.22.59.29	TCP	62	31-11	>	6667	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM=1	
17	19.390402	217.22.59.29	192.168.75.134	TCP	60	6667	>	31-11	[RST, ACK]	Seq=2822385511	Ack=1	Win=64240	Len=0		
18	29.390423	192.168.75.134	217.22.59.29	TCP	62	[TCP Port numbers reused]	31-11	>	6667	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM=1
19	29.390813	217.22.59.29	192.168.75.134	TCP	60	6667	>	31-11	[RST, ACK]	Seq=1	Ack=1	Win=64240	Len=0		
20	29.890078	192.168.75.134	217.22.59.29	TCP	62	31-11	>	6667	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM=1	
21	29.891029	217.22.59.29	192.168.75.134	TCP	60	6667	>	31-11	[RST, ACK]	Seq=247270431	Ack=1	Win=64240	Len=0		
22	30.436812	192.168.75.134	217.22.59.29	TCP	62	31-11	>	6667	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM=1	
23	30.437118	217.22.59.29	192.168.75.134	TCP	60	6667	>	31-11	[RST, ACK]	Seq=772513112	Ack=1	Win=64240	Len=0		
24	40.437211	192.168.75.134	217.22.59.29	TCP	62	[TCP Port numbers reused]	31-11	>	6667	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM=1
25	40.437507	217.22.59.29	192.168.75.134	TCP	60	6667	>	31-11	[RST, ACK]	Seq=1	Ack=1	Win=64240	Len=0		
26	40.936920	192.168.75.134	217.22.59.29	TCP	62	31-11	>	6667	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM=1	
27	40.937326	217.22.59.29	192.168.75.134	TCP	60	6667	>	31-11	[RST, ACK]	Seq=991562453	Ack=1	Win=64240	Len=0		
28	41.483612	192.168.75.134	217.22.59.29	TCP	62	31-11	>	6667	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM=1	
29	41.484018	217.22.59.29	192.168.75.134	TCP	60	6667	>	31-11	[RST, ACK]	Seq=970798576	Ack=1	Win=64240	Len=0		