Analysis Report

FOR SAMPLE2.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

General Information

- File Name   : Sample2.exe
- MD5   : f0cf91991966cf57c207e24fa9ca8afd
- SHA-1   : 12e935c3add1f698098a2d625c98e6f7935b20cd
- Detected as   : TROJ_GEN.R47CCIG
- Other know Aliases   : Backdoor.Win32.IRCBot.faa,
                          Backdoor.Win32.IRCBot.ai009,
                          Win32:IRCBot-DIC [Trj]

Analysis Overview

Sample2.exe was identified as *'TROJ_GEN.R47CCIG'* which is a trojan that connects to an Internet Relay Chat server (IRC server) and provides attacker with remote access to the infected system.

Technical Analysis

- The worm copies itself as ircaddon.exe in system32 directory.
- It modifies and Adds new registry keys to victim machine so that it runs every time Windows starts.
- Tries to spread via attachments sent via messenger services.
- Allows the attacker to gain access and take control of the computer via Internet Relay Chat
- Attacker can perform actions like create, delete or shell execute by sending keywords like "buzz", "sun", "open" etc.
- It tries to connect to the Internet Relay Chat server by making calls via system localhost (i.e. 127.0.0.1) using port no 7777.
- It randomly generates the nickname and user credentials to join the Internet Relay Chat.

```
.data:00449A01 a422          db '422',0           ; DATA XREF: sub_402303+EB↑o
.data:00449A05 ; char a376[4]
.data:00449A05 a376          db '376',0           ; DATA XREF: sub_402303+D7↑o
.data:00449A09 aPongS        db 'PONG %s',0Ah,0   ; DATA XREF: sub_402303+99↑o
.data:00449A12 ; char aPing[]
.data:00449A12 aPing         db 'PING',0          ; DATA XREF: sub_402303+85↑d
.data:00449A17 aNickSUserSNick db 'NICK %s',0Ah   ; DATA XREF: sub_402036+B2↑o
.data:00449A17              db 'USER %s "nick" "%s" :%s',0Ah,0
.data:00449A38 aD_D_D_D      db '%d.%d.%d.%d',0   ; DATA XREF: sub_402036+80↑o
.data:00449A44              db  69h ; i
.data:00449A45 byte_449A45   db 4Ch               ; DATA XREF: sub_401FB9+4A↑r
.data:00449A46 a4zmann3udpem8w db '4zMaNn3uDpEm8wFkOv6PeQlkfAx9dB1tC7GHIJZhKRbSg0TjUcoU5yWrXq2sY',0
.data:00449A84              db  66h ; f
.data:00449A85 byte_449A85   db 41h               ; DATA XREF: sub_401F3C+4A↑r
.data:00449A86 aX9db1tc3udpem8 db 'x9dB1tC3uDpEm8wFk7G-HIJZhKiL4zMaNnOv6PeQlkRbSg0TjUcoU5yWrXq2sY',0
.data:00449AC5              db  4Bh ; K
.data:00449AC6 byte_449AC6   db 69h               ; DATA XREF: sub_401EBF+4A↑r
.data:00449AC7 aL4zmannov6peql db 'L4zMaNnOv6PeQlkfAx9dB1tC3uDpEm8wFk7G-HIJZhRbSg0TjUcoU5yWrXq2sY',0
.data:00449B06 aPrivmsgSS    db 'PRIVMSG %s :%s',0 ; DATA XREF: sub_4014D8+7B6↑o
.data:00449B15 ; char Source[]
.data:00449B15 Source        db 0Ah,0             ; DATA XREF: sub_4014D8:loc_401C40↑o
.data:00449B17 aRedirectSISI db 'redirect %s:%i > %s:%i',0 ; DATA XREF: sub_4014D8+6BF↑o
.data:00449B2E ; char aSend[]
.data:00449B2E aSend         db 'SEND',0          ; DATA XREF: sub_4014D8+631↑o
```

Above is the code excerpt from the Trojan showing auto generation of nick and user credentials to join the Internet Relay Chat

Above is the code excerpt showing the use of keywords to perform certain operations.

System Activity

Registry changes

This worm creates the following registry entries to enable its automatic execution at every system startup under the name *'Internet Messaging File System'*
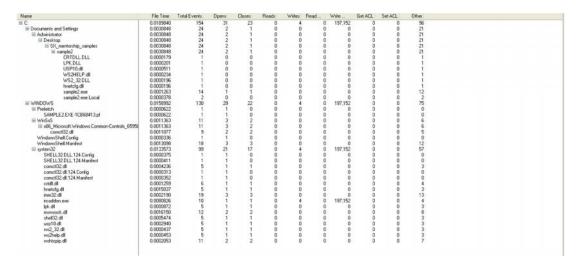
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

The following registry entries are Read
HKLM\SYSTEM\CurrentControlSet\Services\Winsock\Parameters
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\
Catalog_Entries\000000000001

File Changes

It creates a replica of itself at the system folder (system32) with a name ircaddon.exe.
It also modifies \Device\Afd\Endpoint

An Image excerpt from CaptureBat showing registry entries

Network Activity

The Trojan tries to connect to the Internet Relay Chat server by making calls via system localhost (i.e. 127.0.0.1) using port no 7777

An image showing the Trojan trying to establish the connection via local host using port no 7777

An image showing IRC credentials being sent over by the Trojan via port 7777.