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

"A Trojan horse, or Trojan, is a non-self-replicating type of malware which appears to perform a desirable function but instead facilitates unauthorized access to the user's computer system"

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.

Introduction and Technical Analysis

```
.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↑o
.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 '4zMaNn3uDpEm8wFkOv6PeQ1kfAx9dB1tC7GHIJZhKRbSg0TjUcoV5yWrXq2sY',0
.data:00449A84                 db  66h ; f
.data:00449A85 byte_449A85     db 41h                  ; DATA XREF: sub_401F3C+4A↑r
.data:00449A86 aX9db1tc3udpem8 db 'x9dB1tC3uDpEm8wFk7G-HIJZhKiL4zMaNnOv6PeQ1kRbSg0TjUcoV5yWrXq2sY',0
.data:00449AC5                 db  4Bh ; K
.data:00449AC6 byte_449AC6     db 69h                  ; DATA XREF: sub_401EBF+4A↑r
.data:00449AC7 aL4zmannov6peq1 db 'L4zMaNnOv6PeQ1kfAx9dB1tC3uDpEm8wFk7G-HIJZhRbSg0TjUcoV5yWrXq2sY',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'*

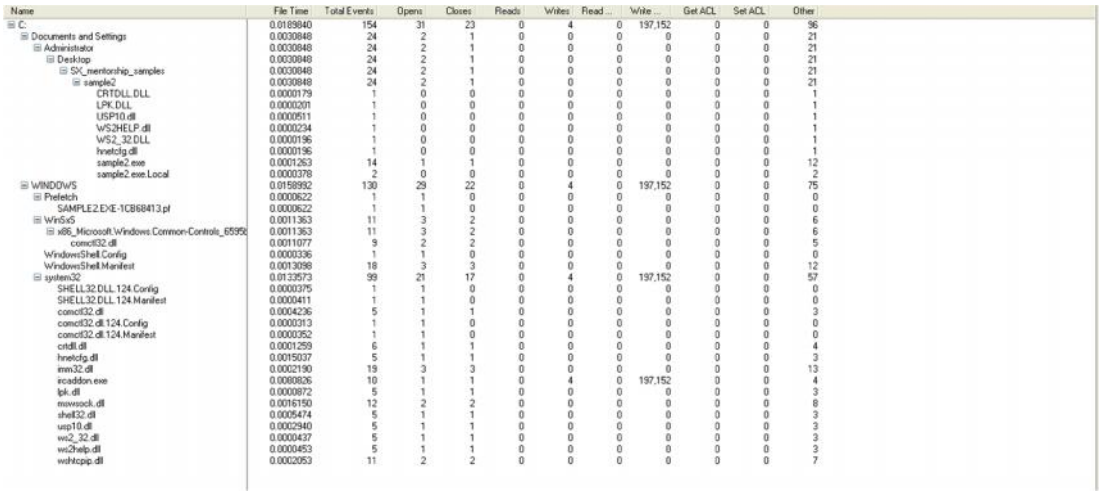
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

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

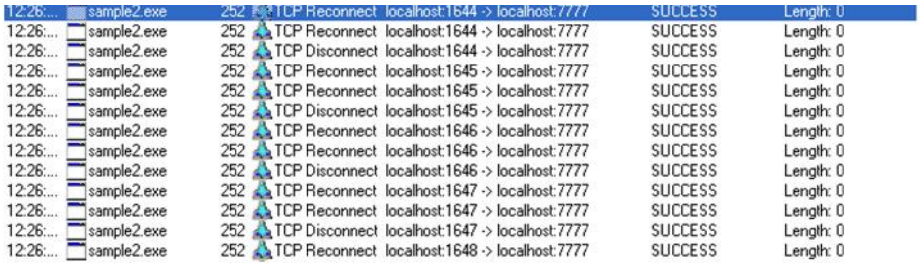


Name	File Time	Total Events	Opens	Closes	Reads	Writes	Read ...	Write ...	Get ACL	Set ACL	Other
C:	0.0189840	154	31	23	0	4	0	197,152	0	0	96
Documents and Settings	0.0030848	24	2	1	0	0	0	0	0	0	21
Administrator	0.0030848	24	2	1	0	0	0	0	0	0	21
Desktop	0.0030848	24	2	1	0	0	0	0	0	0	21
SK_mentorship_samples	0.0030848	24	2	1	0	0	0	0	0	0	21
sample2	0.0030848	24	2	1	0	0	0	0	0	0	21
CRTDLL.DLL	0.0000179	1	0	0	0	0	0	0	0	0	1
LPK.DLL	0.0000201	1	0	0	0	0	0	0	0	0	1
USP10.dll	0.0000511	1	0	0	0	0	0	0	0	0	1
WS2HELP.dll	0.0000234	1	0	0	0	0	0	0	0	0	1
WS2_32.DLL	0.0000196	1	0	0	0	0	0	0	0	0	1
hnetcfg.dll	0.0000196	1	0	0	0	0	0	0	0	0	1
sample2.exe	0.0001263	14	1	1	0	0	0	0	0	0	12
sample2.exe.Local	0.0000378	2	0	0	0	0	0	0	0	0	2
WINDOWS	0.0158992	130	29	22	0	4	0	197,152	0	0	75
Prefetch	0.0000622	1	1	0	0	0	0	0	0	0	0
SAMPLE2.EXE-1CB68413.pf	0.0000622	1	1	0	0	0	0	0	0	0	0
WinSxS	0.0011363	11	3	2	0	0	0	0	0	0	6
x86_Microsoft.Windows.Common-Controls_6595	0.0011363	11	3	2	0	0	0	0	0	0	6
comctl32.dll	0.0011077	9	2	2	0	0	0	0	0	0	5
WindowsShell.Config	0.0000336	1	1	0	0	0	0	0	0	0	0
WindowsShell.Manifest	0.0013098	18	3	3	0	0	0	0	0	0	12
system32	0.0133573	99	21	17	0	4	0	197,152	0	0	57
SHELL32.DLL.124.Config	0.0000375	1	1	0	0	0	0	0	0	0	0
SHELL32.DLL.124.Manifest	0.0000411	1	1	0	0	0	0	0	0	0	0
comctl32.dll	0.0004236	5	1	1	0	0	0	0	0	0	3
comctl32.dll.124.Config	0.0000313	1	1	0	0	0	0	0	0	0	0
comctl32.dll.124.Manifest	0.0000352	1	1	0	0	0	0	0	0	0	0
crtdll.dll	0.0001259	6	1	1	0	0	0	0	0	0	4
hnetcfg.dll	0.0015037	5	1	1	0	0	0	0	0	0	3
imm32.dll	0.0002190	19	3	3	0	0	0	0	0	0	13
ircaddon.exe	0.0080826	10	1	1	0	4	0	197,152	0	0	4
lpk.dll	0.0000872	5	1	1	0	0	0	0	0	0	3
mswsock.dll	0.0016150	12	2	2	0	0	0	0	0	0	8
shell32.dll	0.0005474	5	1	1	0	0	0	0	0	0	3
usp10.dll	0.0002940	5	1	1	0	0	0	0	0	0	3
ws2_32.dll	0.0000437	5	1	1	0	0	0	0	0	0	3
ws2help.dll	0.0000453	5	1	1	0	0	0	0	0	0	3
wshtcpip.dll	0.0002053	11	2	2	0	0	0	0	0	0	7

Network Activity

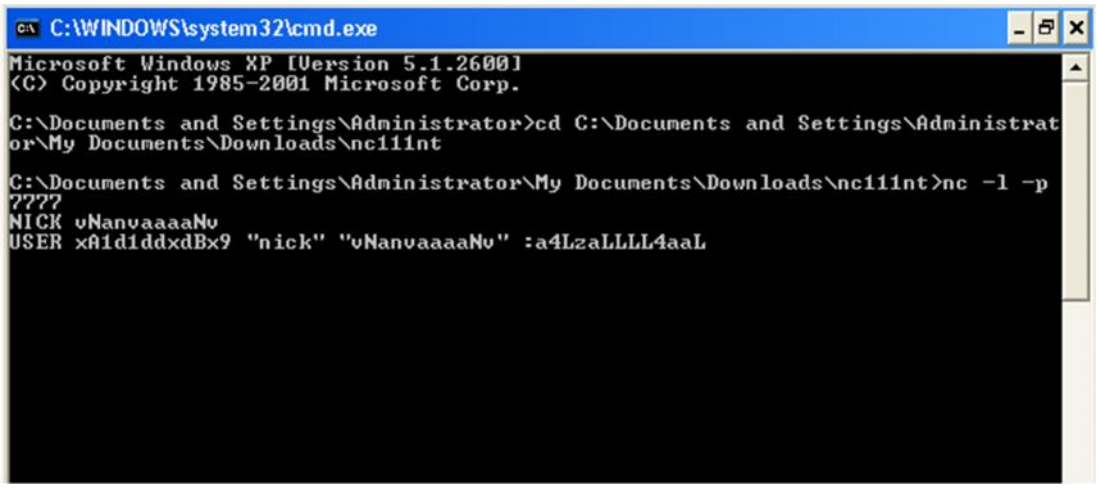
The Trojan tries to connect to the Internet Relay Chat server by making calls via system localhost (i.e. 127.0.0.1) using port no 7777

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



12:26:...	sample2.exe	252	TCP Reconnect	localhost:1644 -> localhost:7777	SUCCESS	Length: 0
12:26:...	sample2.exe	252	TCP Reconnect	localhost:1644 -> localhost:7777	SUCCESS	Length: 0
12:26:...	sample2.exe	252	TCP Disconnect	localhost:1644 -> localhost:7777	SUCCESS	Length: 0
12:26:...	sample2.exe	252	TCP Reconnect	localhost:1645 -> localhost:7777	SUCCESS	Length: 0
12:26:...	sample2.exe	252	TCP Reconnect	localhost:1645 -> localhost:7777	SUCCESS	Length: 0
12:26:...	sample2.exe	252	TCP Disconnect	localhost:1645 -> localhost:7777	SUCCESS	Length: 0
12:26:...	sample2.exe	252	TCP Reconnect	localhost:1646 -> localhost:7777	SUCCESS	Length: 0
12:26:...	sample2.exe	252	TCP Reconnect	localhost:1646 -> localhost:7777	SUCCESS	Length: 0
12:26:...	sample2.exe	252	TCP Disconnect	localhost:1646 -> localhost:7777	SUCCESS	Length: 0
12:26:...	sample2.exe	252	TCP Reconnect	localhost:1647 -> localhost:7777	SUCCESS	Length: 0
12:26:...	sample2.exe	252	TCP Reconnect	localhost:1647 -> localhost:7777	SUCCESS	Length: 0
12:26:...	sample2.exe	252	TCP Disconnect	localhost:1647 -> localhost:7777	SUCCESS	Length: 0
12:26:...	sample2.exe	252	TCP Reconnect	localhost:1648 -> localhost:7777	SUCCESS	Length: 0

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



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>cd C:\Documents and Settings\Administrat
or\My Documents\Downloads\nc111nt

C:\Documents and Settings\Administrator\My Documents\Downloads\nc111nt>nc -l -p
7777
NICK vNanvaaaaNv
USER xA1d1ddxdBx9 "nick" "vNanvaaaaNv" :a4LzaLLLL4aaL
```