Brute Forcing with DLL Injection

2010-11-22

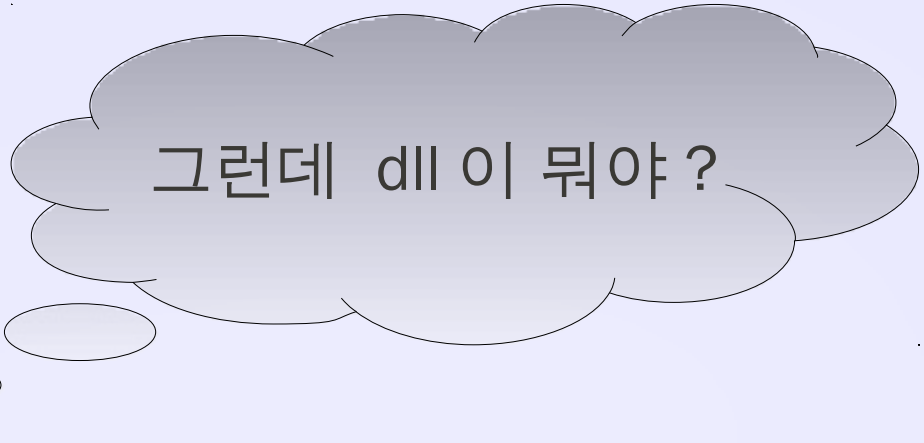
김 연재 (Yeonjae Kim)

CERT-IS

6l4ck3y3 at gmail.com
http://hisjournal.net

순서

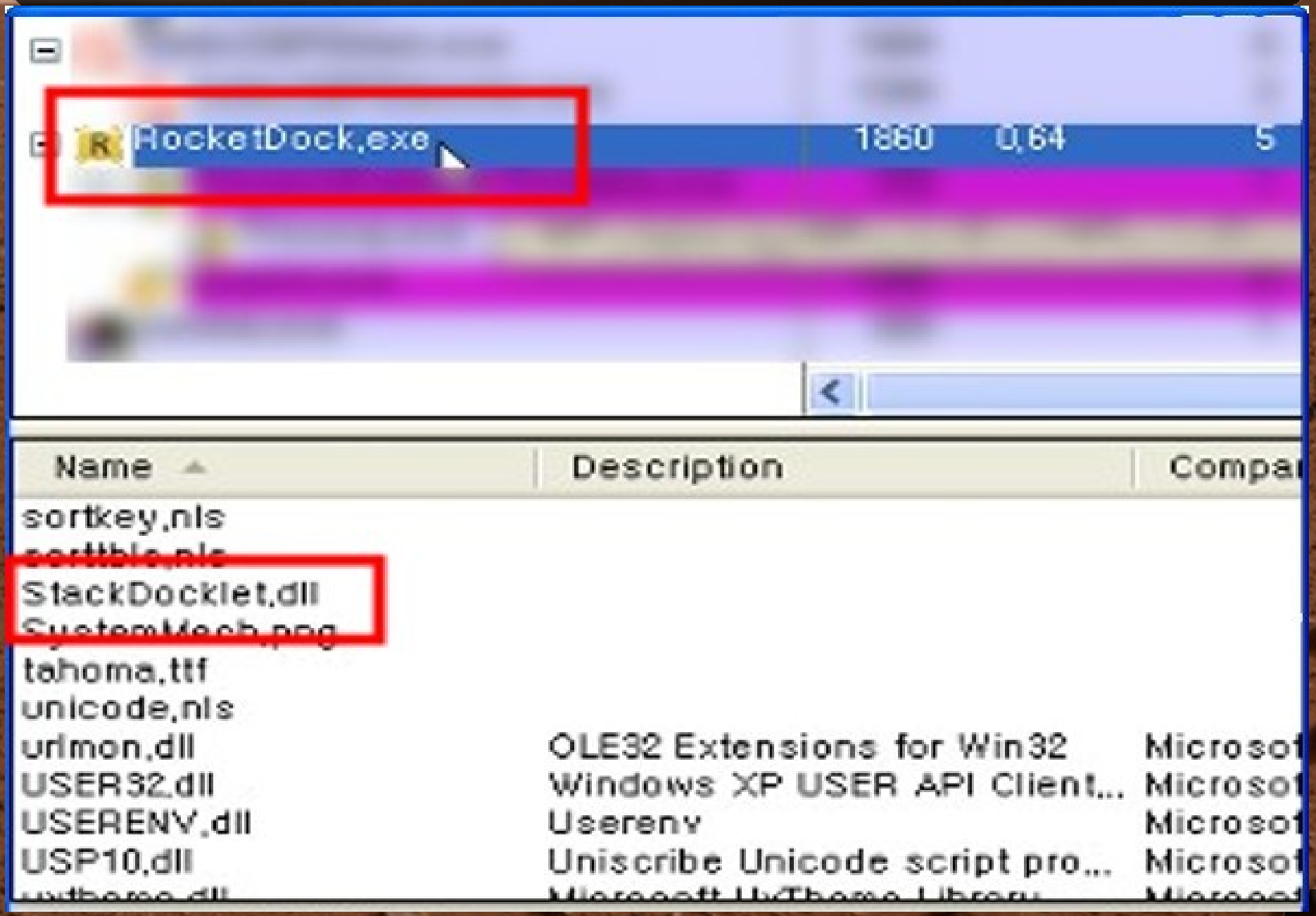
- 왜 DLL 을 삽입하는가 ?
- DLL Injection 을 어떻게 하는가 ?
- 암호화 루틴을 역이용하자 .
  - Demo
- Brute Force (무차별 대입 공격)
  - Demo



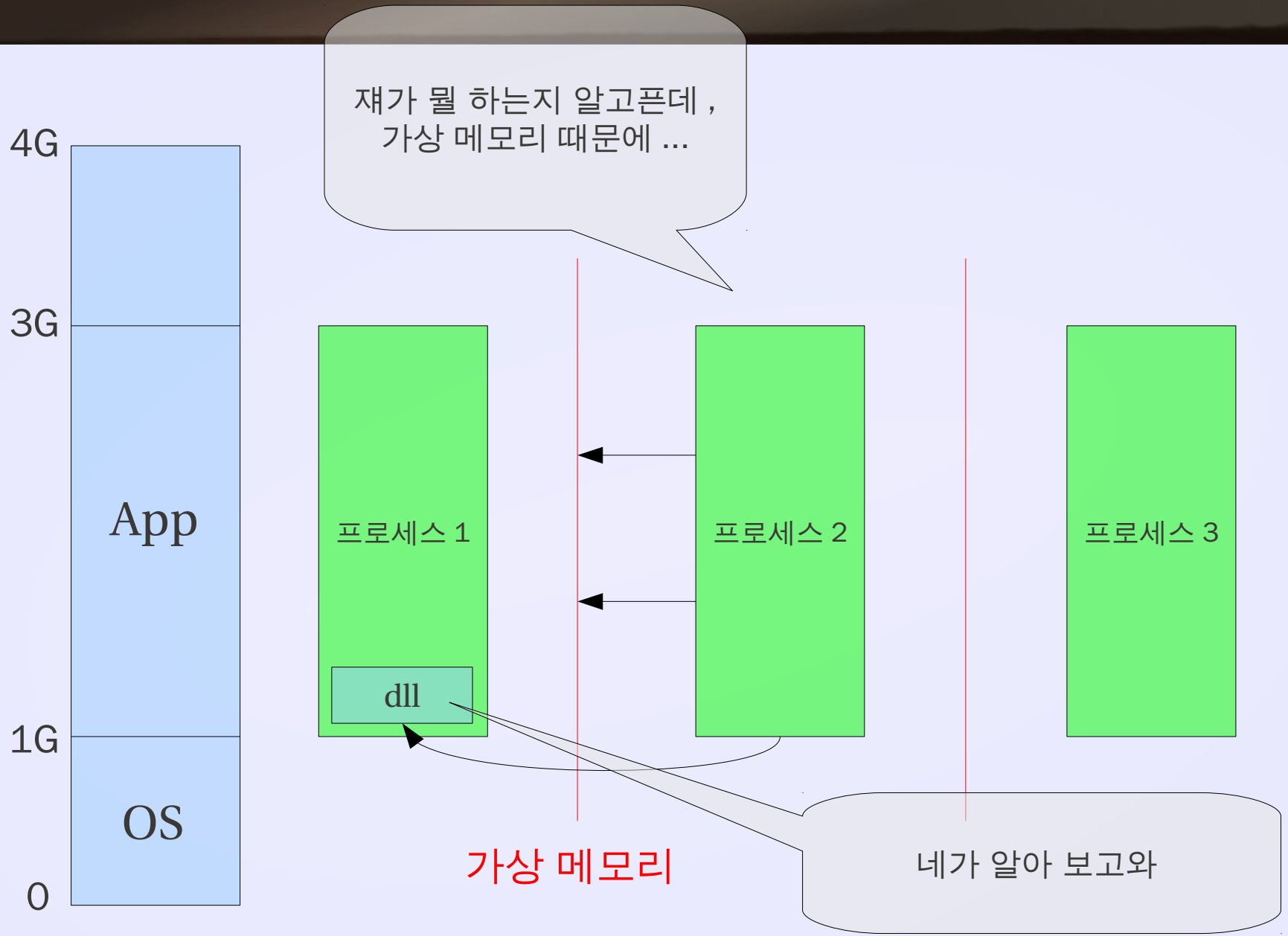
왜 **DLL** 을 삽입하는가 **?**

왜 DLL 을 삽입하는가 ?

왜 DLL 을 삽입하는가 ?


RocketDock.exe
1860
0.64
5
Name
Description
sortkey.nls
StackDocklet.dll
tahoma.ttf
unicode.nls
urlmon.dll
OLE32 Extensions for Win32
USER32.dll
Windows XP USER API Client...
USERENV.dll
Userenv
USP10.dll
Uniscribe Unicode script pro...

왜 DLL 을 삽입하는가 ?


재가 뭘 하는지 알고픈데 ,
가상 메모리 때문에 ...
4G
3G
1G
0
App
OS
프로세스 1
dll
프로세스 2
프로세스 3
가상 메모리
네가 알아 보고와

DLL Injection 을 어떻게 하는가?

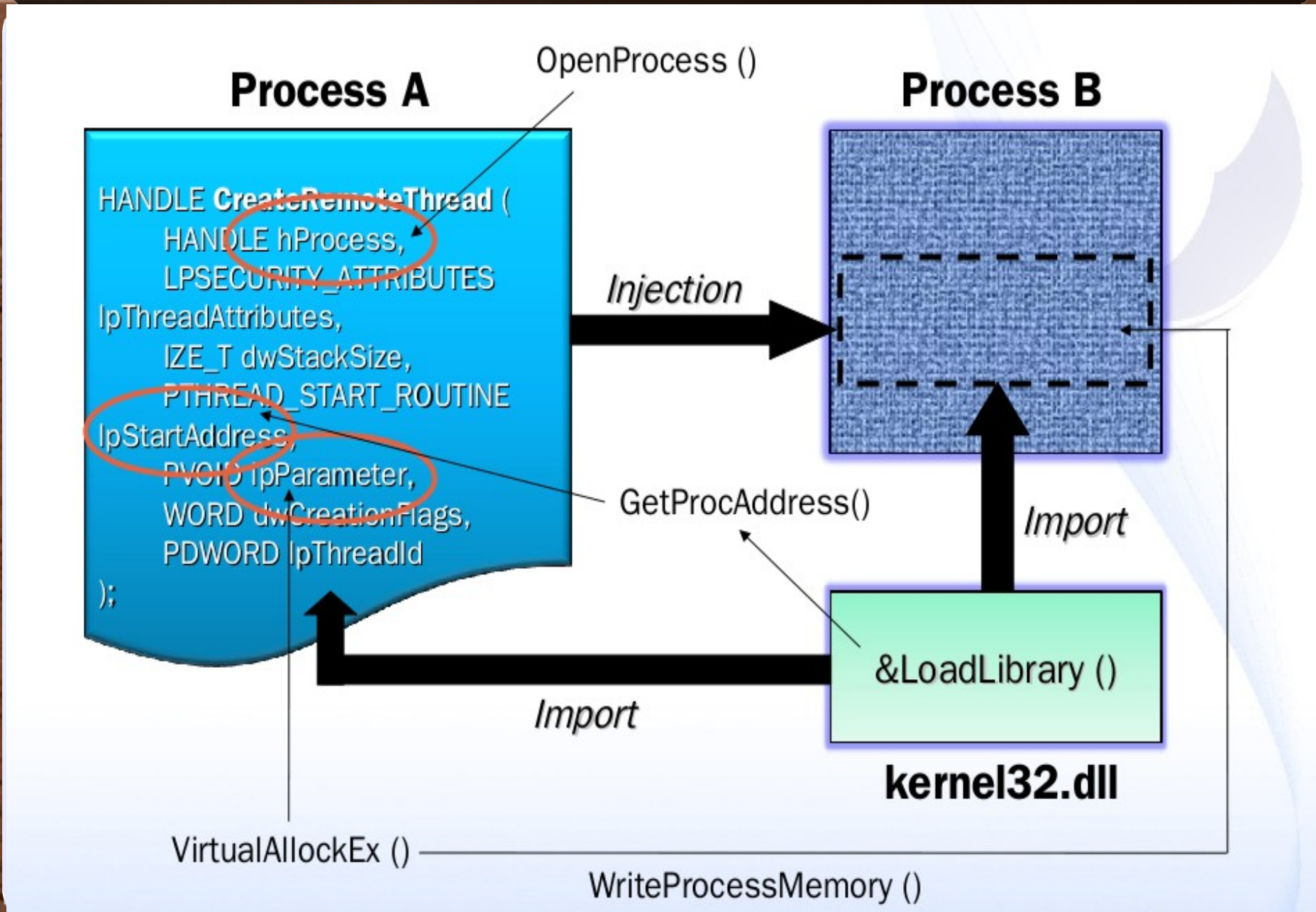
DLL Injection 을 어떻게 하는가 ?

<table>
<tr><th>Method</th><th>Object
(what)</th><th>Location
(where)</th><th colspan="2">Technique
(how)</th><th>API</th></tr>
<tr><td>static</td><td>File</td><td rowspan="5">1) IAT
2) Code
3) EAT</td><td colspan="2">X</td><td>X</td></tr>
<tr><td rowspan="4">dynamic</td><td rowspan="4">Process
Memory

00000000
~
7FFFFFFF</td><td colspan="2">A) Debug
(Interactive)</td><td>DebugActiveProcess
GetThreadContext
SetThreadContext</td></tr>
<tr><td rowspan="3">B) Injection
(stand
alone)</td><td>B-1)
Independant
Code</td><td>CreateRemoteThread</td></tr>
<tr><td rowspan="2">B-2) DLL file</td><td>Registry (AppInit_DLLs)
BHO (IE only)</td></tr>
<tr><td>SetWindowsHookEx
CreateRemoteThread</td></tr>
</table>

API Hooking Tech Map

DLL Injection 을 어떻게 하는가 ?



DLL Injection 을 어떻게 하는가 ?

```
#1. hProcess = OpenProcess (PROCESS_ALL_ACCESS, FALSE, dwPID);
```

- DLL 을 삽입할 프로세스의 핸들을 구함
  - dwPID 는 프로세스의 PID (Process ID) 값

DLL Injection 을 어떻게 하는가 ?

```
#2. lpParameter = VirtualAllocEx (hProcess, NULL, dwBufSize,
                                  MEM_COMMIT, PAGE_READWRITE);
```

- 대상 프로세스 메모리 공간에 버퍼를 할당
  - hProcess 를 인자로 사용
  - dwBufSize 는 strlen(DLL 의 경로) + 1
- Debug API

DLL Injection 을 어떻게 하는가 ?

```
#3. WriteProcessMemory (hProcess, lpParameter, (LPVOID)szDllName,
dwBufSize, NULL);
```

- 대상 프로세스에 할당한 버퍼에 DLL 의 경로를 씀
  - hProcess, lpParameter 를 인자로 사용
  - szDllName 은 DLL 의 경로
  - dwBufSize 는 strlen(DLL 의 경로) + 1
- Debug API

DLL Injection 을 어떻게 하는가 ?

```
#4. lpStartAddress = (LPTHREAD_START_ROUTINE)
                     GetProcAddress (hMod, "LoadLibraryA");
```

- kernel32.dll 내부의 LoadLibraryA 함수의 주소를 구함
  - hMod 는 GetModuleHandle ("kernel32.dll") 로 구함
  - LoadLibraryA 는 DLL 을 호출하는 API
- Windows 는 핵심 DLL 의 가상 주소를 동일하게 관리
  - 프로세스 1 과 프로세스 2 의 kernel32.dll 의 가상 주소가 동일하다는 의미

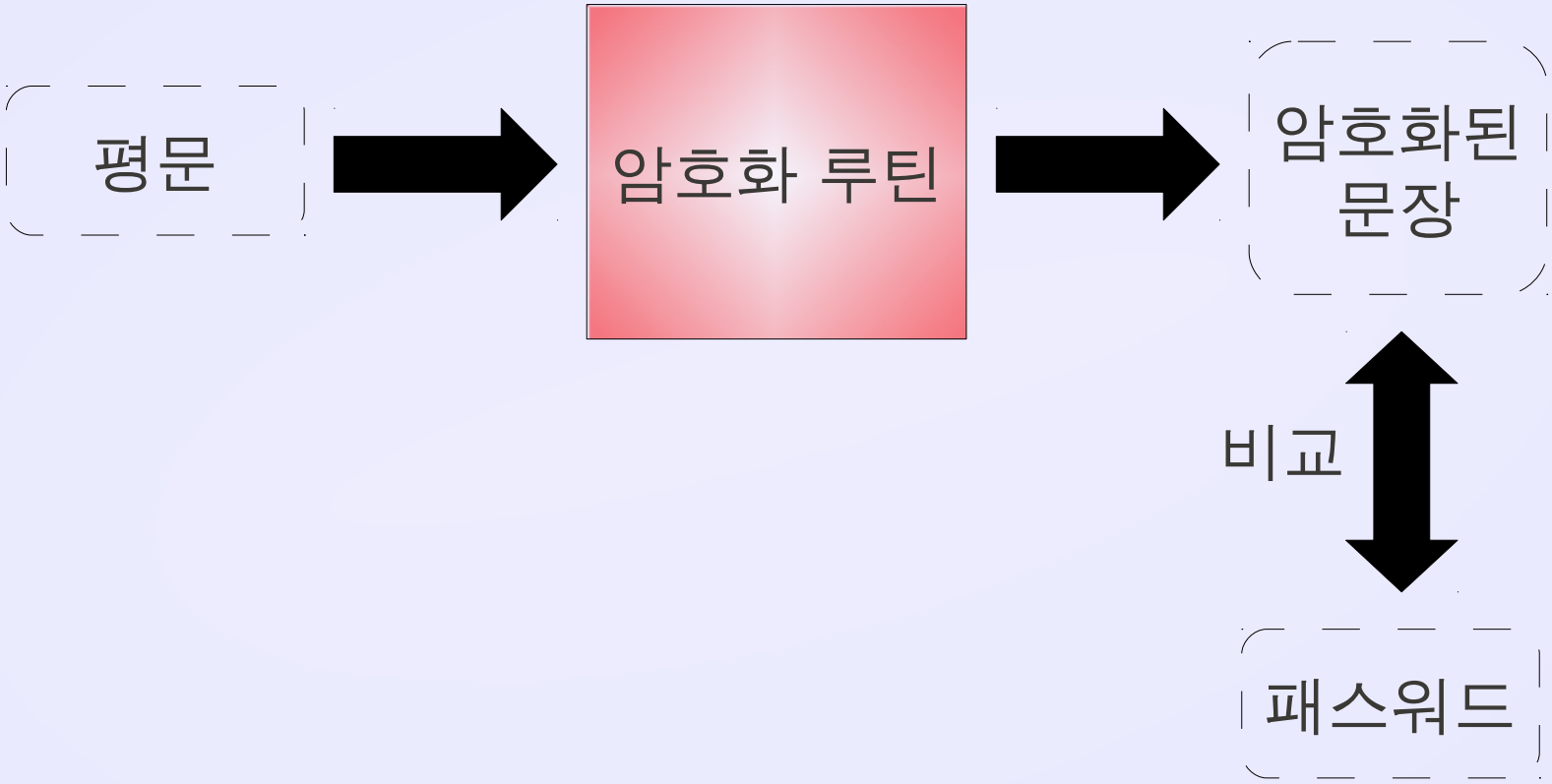
DLL Injection 을 어떻게 하는가 ?

```
#5. hThread = CreateRemoteThread (hProcess, NULL, 0, lpStartAddress,
                                  lpParameter, 0, NULL);
```

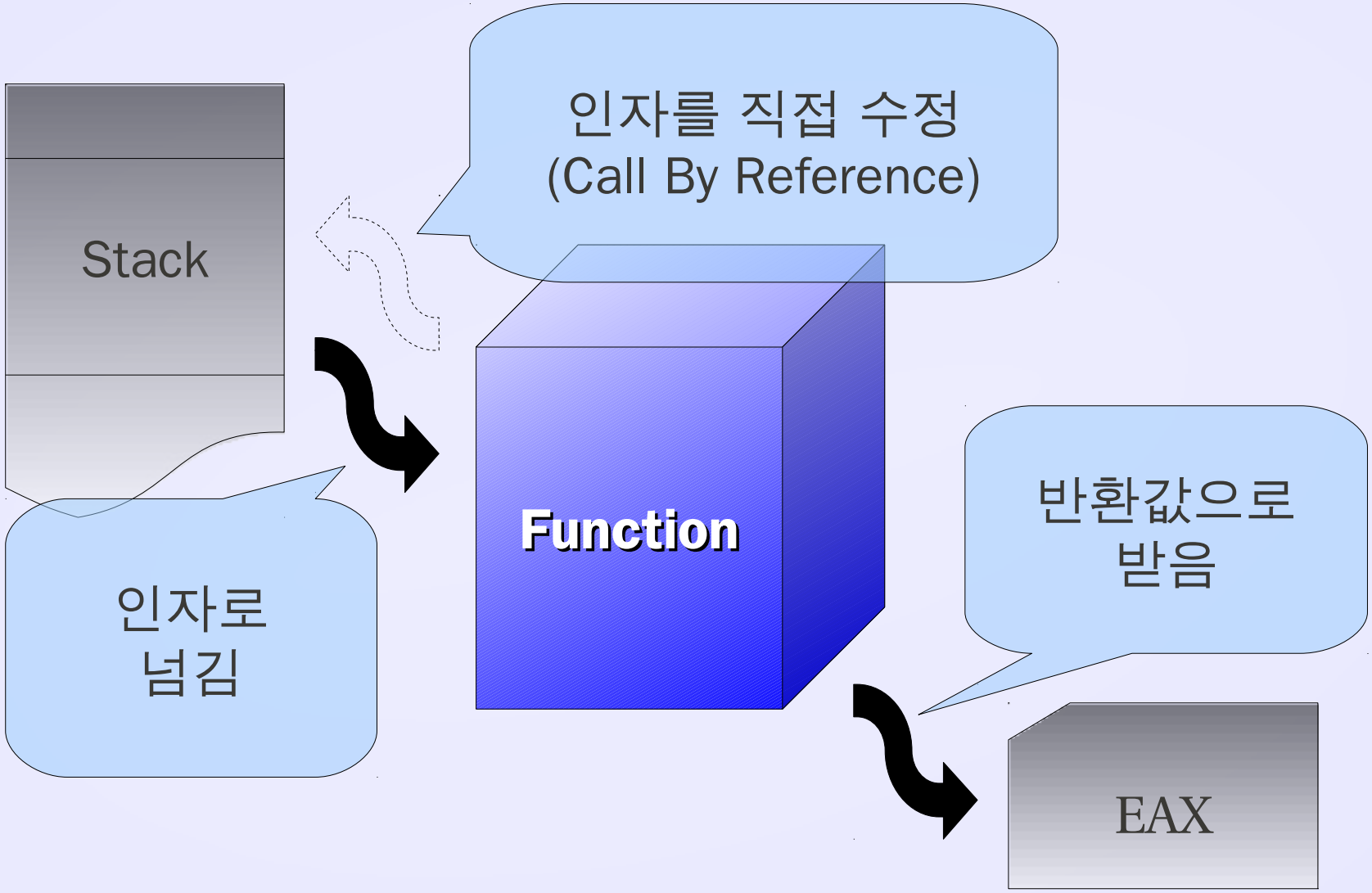
- 대상 프로세스에게 LoadLibraryA 를 호출하여 ,
  lpParameter 에 쓰여진 경로의 DLL 을 부르도록 지시

암호화 루틴을 역이용하자..

암호화 루틴을 역이용하자 .



암호화 루틴을 역이용하자 .

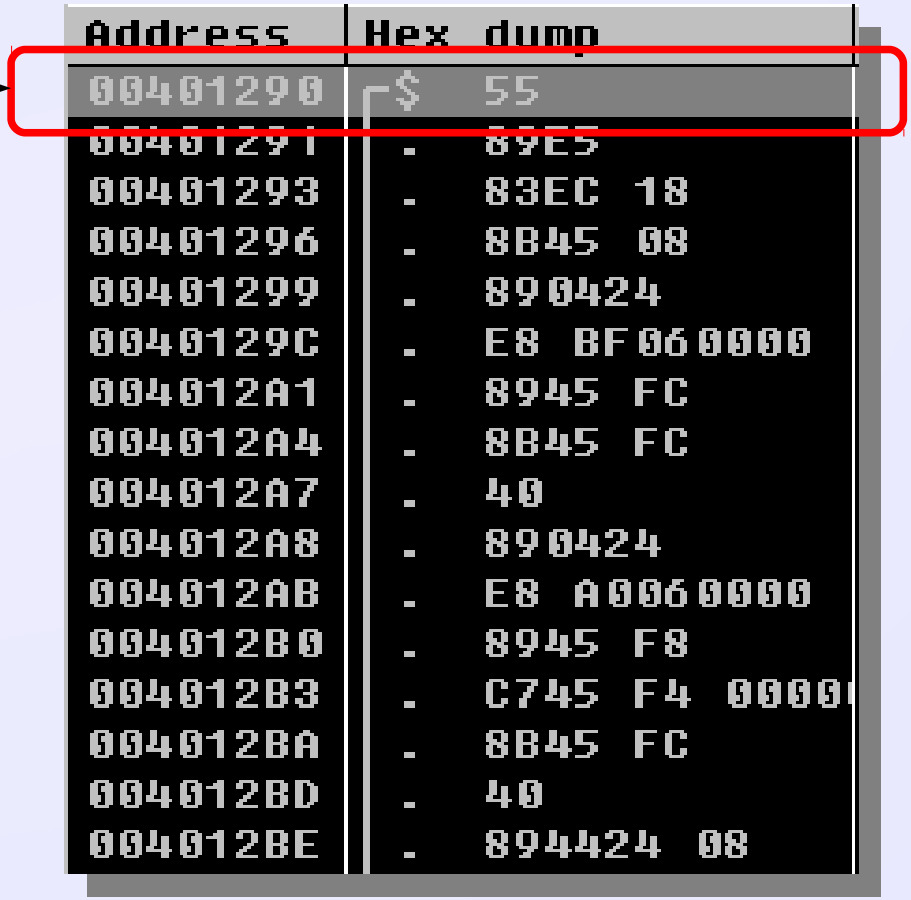


Demo 1 – 암호화 루틴을 찾자

암호화 루틴을 역이용하자.

암호화 루틴

함수 포인터



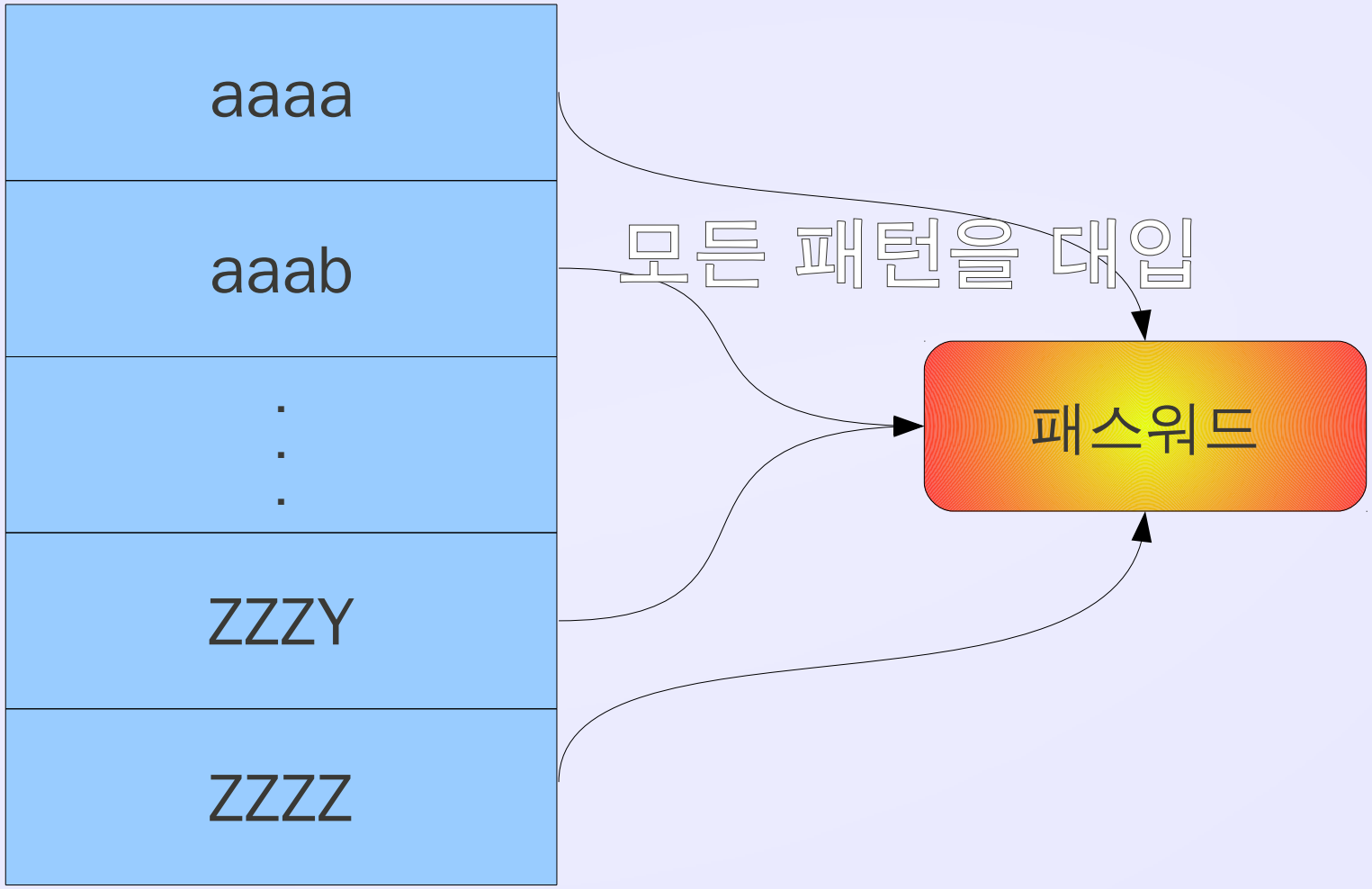
Address	Hex dump
00401290	$ 55
00401291	. 89E5
00401293	. 83EC 18
00401296	. 8B45 08
00401299	. 890424
0040129C	. E8 BF060000
004012A1	. 8945 FC
004012A4	. 8B45 FC
004012A7	. 40
004012A8	. 890424
004012AB	. E8 A0060000
004012B0	. 8945 F8
004012B3	. C745 F4 0000
004012BA	. 8B45 FC
004012BD	. 40
004012BE	. 894424 08

암호화 루틴을 역이용하자.

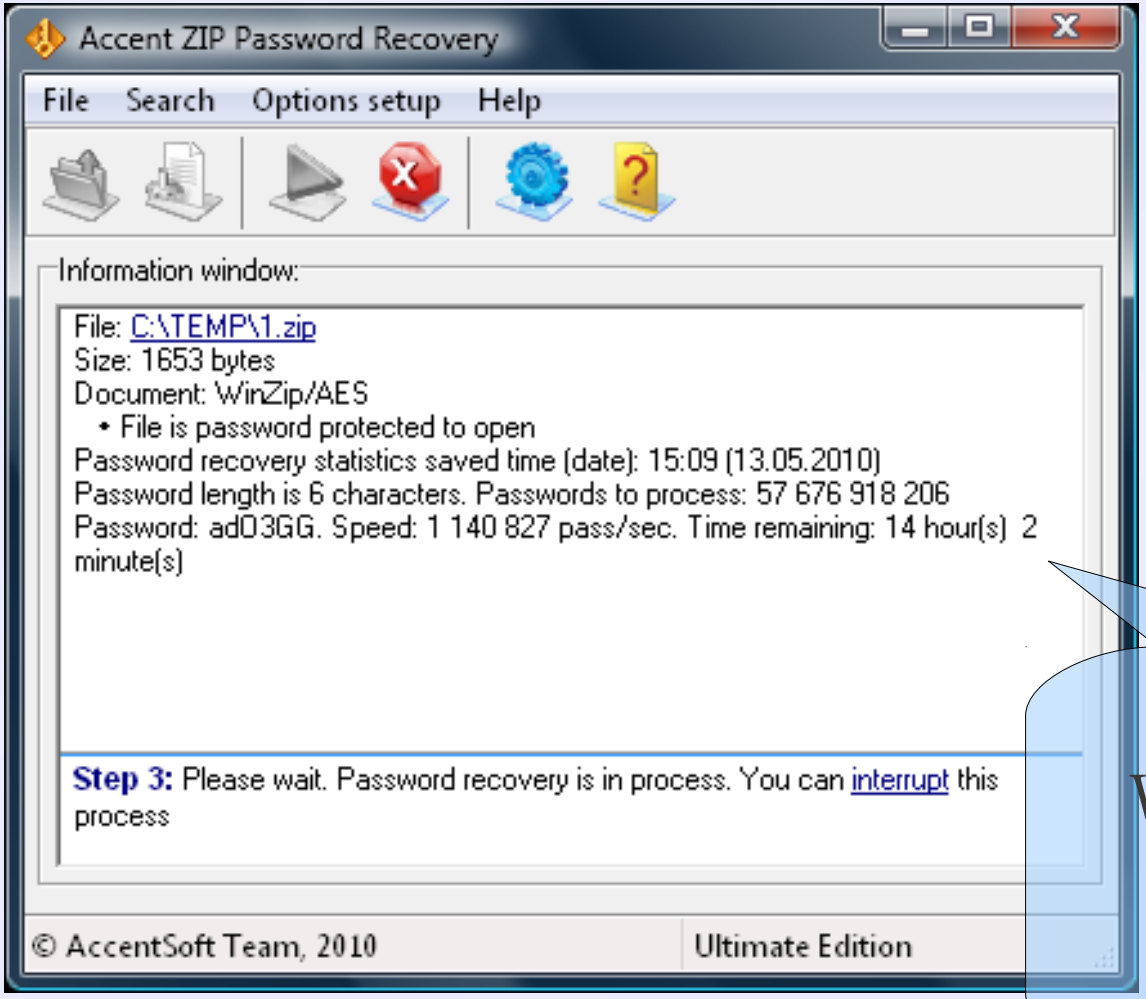
```
// inject-bf.c (DllMain)

typedef char* (*INJECTED_FUNC)(char*);

INJECTED_FUNC GetValue = NULL;
char* retValue = NULL;

GetValue = (INJECTED_FUNC)0x401290;
retValue = GetValue (str);
```

Brute Force (무차별 대입 공격)

Brute Force (무차별 대입 공격)



Brute Force (무차별 대입 공격)



WinZip/AES(128bit)

14 시간 2 분

Brute Force (무차별 대입 공격)

```
// bruteforce.h
#define MIN 1
#define MAX 10
#define CHARSET "abcdefghijklmnopqrstuvwxyz
                 ABCDEFGHIJKLMNOPQRSTUVWXYZ
                 0123456789!@#$%^&*()-_=+[]{}|;:,.<>/?~ "

// bruteforece.c
int finished (char* block, char* charset, char* templ);
void increment (char* block, int len,
                char* charset, char* templ);
void chunk (int start, int end,
            char* charset, char* templ, char* startblock);
int StartBrute (int min, int max);
```

Demo 2 – 무차별 대입 공격

질문 ??

Questions ??
Comments ??
Ideas ??
email me

6l4ck3y3 at gmail.com
http://hisjournal.net/blog

Thanks