Armadillo/Asprotect/Themida & HackShield Option/AntiCpX/LMP 2.0 호환성 테스트 결과

- **Amazon Test Client** Ver. : 5.5.18.1(Build 192)
- **Armadillo** Ver. : v.6.4.0.640
- **Asprotect** Ver. : v.1.4 build 11.20 Release
- **Themida** Ver. : v.2.2.0.0
- **HackShield Option** : SpeedHack, ProcessMemory, KDTracer, OpenProcess, AutoMouse, MessageHook, ProcessScan, DoNotTerminateProcess, LogFile, Allow SvcHost, Allow LSASS, Allow CSRSS,

1. Packer & HackShield Option/AntiCpX/LMP2.0 호환성 결과

Packer	Packer Option	HackShield Option과 호환성 여부	HackShield 확장서버 연동과 호환성 여부	HackShield LMP 2.0과 호환성 여부	비 고
Armadillo	CopyMem-II + Debug-Blocker	X	X	X	
	Standard protection + Debug-Blocker	X	X	X	
	Standard protection only	◎	◎	◎	
	Minimum protection	◎	◎	◎	
	Import Table Elimination	X	X	X	
	Strategic Code Splicing	X	X	X	
	Memory-Patching Protections	◎	◎	◎	
	Nanomities Processing	X	X	X	
Asprotect	Anti-Debugger Protection	◎	X		
	Checksum Protection	◎	X		
	Advanced Import Protection	◎	X		
	Protect Original EntryPoint	◎	X		
	Emulate Standard System Functions	◎	X		
	Resources Protection	◎	X		
	Preserve extra data	◎	X		
	Use Max Compression	◎	X		
Themida	**Anti-Debugger Detection (Advanced)**	◎	◎	◎	
	Anti-Debugger Detection (Ultra)	◎	◎	◎	
	Anti Dumpers	◎	◎	◎	
	Entry Point Obfuscation	◎	◎	◎	
	Resources Encryption	◎	◎	◎	
	Advanced API-Wrapping (disable)	◎	◎	◎	
	Advanced API-Wrapping (Level 1)	◎	X	◎	
	Advanced API-Wrapping Lv1 + ImplicitRedirection[i]	◎	◎	◎	
	Advanced API-Wrapping (Level 2)	◎	X	◎	
	Advanced API-Wrapping Lv2 + Implicit Redirection	◎	◎	◎	
	Anti-Patching (None)	◎	◎	◎	
	Anti-Patching (File Patching)	◎	◎	◎	
	Anti-Patching (Sign Support)	◎	◎	◎	
	Metamorph Security	◎	◎	◎	

	Memory Guard	◎	◎	◎	
	Compression	◎	◎	◎	
	Encrypt Application	◎	◎	◎	
XBundler	Make file visible to OpenDialog	◎	◎	◎	
	GetPrivateProfile APIs support	◎	◎	◎	
	Allow bundling from any directory	◎	◎	◎	
	AVI files support	◎	◎	◎	
	Deleted extracted on exit	◎	◎	◎	

◎ : 호환 가능, X : 호환 불가능

※ 위 리스트에 명시되지 않은 항목에 대해서는 핵쉴드와의 호환성을 보증하지 못합니다.

2. Windows XP에서 패킹한 Amazon.exe를 타 OS에서 실행했을 때 메모리 Code Section 비교결과

	Windows 98	Windows 2000	WindowsServer2003	Windows XP	Windows Vista
Armadilllo[ii]	◎	◎	◎	◎	◎
Asprotect[iii]	X	X	X	X	X
Themida	X	X	X	◎	X
Themida + ImplicitRedirection	◎	◎	◎	◎	◎
XBundler + ImplicitRedirection	◎	◎	◎	◎	◎

◎ : OS에 따라 Binary 변경 되지 않음. X : OS에 따라 Binary 변경됨

A. Windows XP에서의 Test는 동일한 binary를 5회 실행 시, **Code Section**내의 수정 여부를 확인.

B. Themida + ImplicitRedirection을 사용하면 Binary 내 Code Section이 수정되지 않음.
(ImplicitRedirection 옵션을 적용 안 하면 LMP나 핵쉴드 서버연동의 메모리검사 등의 일부 기능에서 오진이 생길 수 있습니다.)

C. 핵쉴드는 자체적으로 Dump생성에 대한 부분을 차단하고 있지 않습니다.
- 단, 핵쉴드 보호차원에서 사용하는 패커인 Themida와의 내부이슈로 인해 **_AhnHS_Initialize 이후 SetUnhandledExceptionFilter** 설정을 해 주시면 Dump생성이 되는 것을 확인 가능합니다.
- 예제는 아래와 같습니다.

```
ex )
_AhnHS_Initialize()
_AhnHS_StartService()
__try
{
....
}
__except

or

_AhnHS_Initialize()
_AhnHS_StartService()
SetUnhandledExceptionFilter()
-
```

[i] 옵션을 활성화하기 위해서는 http://www.oreans.com/Release/ThemidaINI.zip 를 다운로드 받아 Themida가 설치된 폴

더에 풀고 실행하면 나타나는 SecureEngine Config 메뉴에 있습니다.

[ii] Standard Protection + Minimum Protection + Memory-Patching Protections

[iii] 모든 옵션 적용 안 됨.