

# Armadillo/Asprotect/Themida & HackShield Option/AntiCpX/LMP 2.0

## Compatibility Result

- **Amazon Test Client** Ver. : 5.5.5.1 (Build 119)
- **Armadillo** Ver. : v.6.4.0.640
- **Asprotect** Ver. : v.1.4 build 11.20 Release
- **Themida** Ver. : v.2.1.7.0
- **HackShield Option** : SpeedHack, ProcessMemory, KDTracer, OpenProcess, AutoMouse, MessageHook, ProcessScan, DoNotTerminateProcess, LogFile, Allow SvcHost, Allow LSASS, Allow CSRSS,

### 1. Packer & HackShield Option/AntiCpX/LMP2.0 Compatibility Result

Packer	Packer Option	Compatibility with HackShield Option	Compatibility with HackShield ESSD	Compatibility with HackShield LMP 2.0	Note
Armadillo	CopyMem-II + Debug-Blocker	X	X	X	
	Standard protection + Debug-Blocker	X	X	X	
	<b>Standard protection only</b>	⊙	⊙	⊙	
	<b>Minimum protection</b>	⊙	⊙	⊙	
	Import Table Elimination	X	X	X	
	Strategic Code Splicing	X	X	X	
	<b>Memory-Patching Protections</b>	⊙	⊙	⊙	
	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	<b>Anti-Debugger Detection (Advanced)</b>	⊙	⊙	⊙	
	<b>Anti-Debugger Detection (Ultra)</b>	⊙	⊙	⊙	
	<b>Anti Dumpers</b>	⊙	⊙	⊙	
	<b>Entry Point Obfuscation</b>	⊙	⊙	⊙	
	<b>Resources Encryption</b>	⊙	⊙	⊙	
	<b>Advanced API-Wrapping (disable)</b>	⊙	⊙	⊙	
	Advanced API-Wrapping (Level 1)	⊙	X	⊙	
	<b>Advanced API-Wrapping Lv1 + ImplicitRedirection<sup>i</sup></b>	⊙	⊙	⊙	
	Advanced API-Wrapping (Level 2)	⊙	X	⊙	
	<b>Advanced API-Wrapping Lv2 + Implicit Redirection</b>	⊙	⊙	⊙	
	<b>Anti-Patching (None)</b>	⊙	⊙	⊙	
	<b>Anti-Patching (File Patching)</b>	⊙	⊙	⊙	
	<b>Anti-Patching (Sign Support)</b>	⊙	⊙	⊙	

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

⊙ : Compatible, X : Incompatible

※ Complete compatibility is not guaranteed. Only the features listed in the table above are supported.

## 2. Comparison table of memory code section when running Amazon.exe (Windows XP-packed) on OS other than Windows XP

	Windows 98	Windows 2000	WindowsServer2003	Windows XP	Windows Vista
Armadillo <sup>ii</sup>	⊙	⊙	⊙	⊙	⊙
Asprotect <sup>iii</sup>	X	X	X	X	X
Themida	X	X	X	⊙	X
Themida + ImplicitRedirection	⊙	⊙	⊙	⊙	⊙
XBundler + ImplicitRedirection	⊙	⊙	⊙	⊙	⊙

⊙ : Binary is not modified regardless of OS. X : Binary is modified due to OS

A test on Windows XP was executed 5 times to check for any modification in the code section memory. When using Themida with ImplicitRedirection option, the code section memory in the binary did not get modified. (If ImplicitRedirection option is not used, there may be a false-positive in HackShield LMP or HackShield Server Side Detection.)

- HackShield does not block the creation of dump files. However, a packer called Themida, which is used to enhance the security of HackShield, blocks it. Hence, **SetUnhandledExceptionFilter ()** must be used just after **\_AhnHS\_Initialize() & \_AhnHS\_StartService()** to create a dump file. The following sample code will be helpful.

```

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

or

_AhnHS_Initialize(
_AhnHS_StartService();
SetUnhandledExceptionFilter()
-

```

<sup>i</sup> To enable options, download <http://www.oreans.com/Release/ThemidaINI.zip> and extract it to the folder where Themida is installed. When executing Themida, the options will be available in SecureEngine Config menu.

- 
- ii Standard Protection + Minimum Protection + Memory-Patching Protections
  - iii Not all options are applied.