



# Stories From The DRM World: The Settec Case

Elia Florio  
Symantec Security Response, Dublin

*Originally published by Virus Bulletin, April 2006. Copyright held by Virus Bulletin, Ltd., but is made available courtesy of Virus Bulletin. For more information on Virus Bulletin, please visit <http://virusbtn.com/>*



# Stories From The DRM World: The Settec Case

## Contents

The Settec Case.....	4
Strange Setup.....	5
The Protection Scheme.....	6
What Are The Real Risks?.....	7
Competitive Antagonism In Legitimate Software.....	9
Conclusions.....	9
References.....	10
About the Author.....	10

Months after Sony got into trouble for using rootkit functionality in the DRM protection of audio media, the word 'rootkit' is still hitting the headlines. This time the trouble comes in the form of DVD movies containing DRM software from Settec.

In 2001: A Space Odyssey, the legendary computer HAL 9000 was built for the purpose of supporting the astronauts and their mission. Later in the movie, however, the computer revealed an unexpected murderous instinct. Due to an unpredictable programming error, it began to kill the astronauts of the Discovery space ship. HAL 9000 turned abilities that were intended to be used for good purposes against the humans.

The connection between Arthur Clarke's novel and the Settec case is apparent in the use of system hooking, which is a powerful technique that can be used for good or malicious purposes. When this technique is included in software that is installed on users' machines, everyone should be aware of the potential risks. This article will focus principally on the Settec case. I will discuss the security issues of the code implementation, including how it is different from the Sony case.

### The Settec Case

At the end of January 2006, German computer users started to post complaints to a public news-group<sup>[1]</sup> about the DVD of the movie of Mr. & Mrs. Smith. Users had noticed the presence of a new protection system on the DVD, which was essentially based on two levels of security. The first was a physical protection on the disc surface (probably some kind of bad sectors), and the second was software protection installed on the machines by the autorun player. The messages posted on the public forum reported strange errors relating to popular DVD ripping programs in the presence of the aforementioned software. It didn't take long for experienced computer users to understand what was going on.

One week later, the popular German news Web site Heise Online published the first technical analysis of the protection software found on the Mr. & Mrs. Smith DVD, which is named 'Alpha-DVD' and produced by the Korean company Settec<sup>[2]</sup>.



**Figure 1:** The Settec DRM was found first on the German edition of the Mr & Mrs. Smith DVD, but there are many other DVDs that may make use of the same protection scheme.

According to the first analysis, Alpha-DVD was using rootkit-like abilities to hide itself.

## Strange Setup

The Alpha-DVD protection software (version 1.0.3.5) is composed of two modules – an executable file and a DLL library, which have the following characteristics:

**Filename:** %System%\[RANDOM].EXE  
**Size (bytes):** 827.392  
**MD5:** 0x4e7797f813c10cb172b3f219638c8114

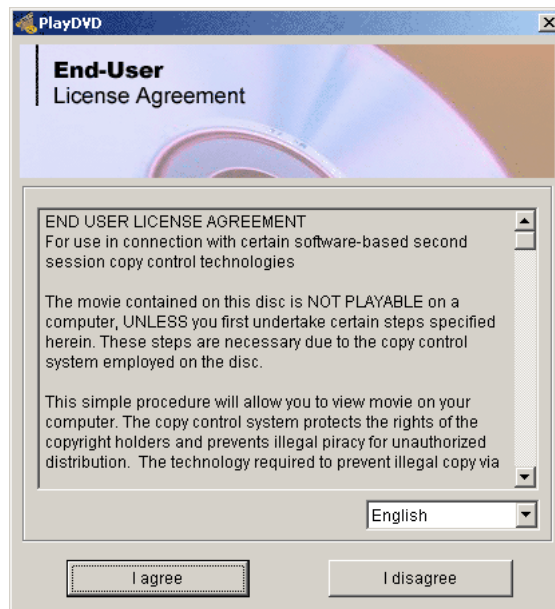
**Filename:** %System%\HADL.DLL  
**Size (bytes):** 356.352  
**MD5:** 0x9b845d8fc0b7e9f7ac5659ca6ba7e079

It is possible to recognize this protection on the DVD by the presence of the main executable under the DVD root folder, with the name 'alpha.dat'. The executable is copied into the %System% folder with a random name, and drops the DLL library once it is executed.

The .EXE file contains several other executables (including a VXD driver for Windows 9X), which are embedded as resources. The HADL.DLL file is located under the 'FILES' tree of the resources table and has the resource number 143.

When a DVD containing Alpha-DVD protection is inserted into the DVD-ROM drive with the autorun feature enabled, 'PlayDVD.EXE' (which is stored on the DVD disc) runs immediately. This file is the main installer of the Settec protection. According to the producer, the first thing the installer does is to display an End User License Agreement (Figure 2), asking users to consent to the installation of the Alpha-DVD program on the system.

Typically, if a user does not agree to the installation process, the program (and its system hooking component) will not be copied onto the machine. However, tests have shown that a copy of the .EXE file and the DLL are saved in the temporary folder of the computer before any consent is given by the user. The setup program copies the executable and the DLL to the following paths before any user interaction:



**Figure 2:** Alpha-DVD protection shows an End User License Agreement window at autorun, however some files are copied onto the users' machines before they agree to the installation process.

```
%Temp%\tmpagent.exe  
%Temp%\hadl.dll
```

When the 'I disagree' button is clicked, the installer ejects the DVD disc and deletes the 'tmpagent.exe' file. However, it does not delete the 'HADL.DLL' library, which remains saved on the system even after reboot.

If this file was a text or image file, it would pose little risk to security. However, this library is the core system hooking component that implements all the hooking code. It would be possible for malicious code to utilize the component unbeknownst to the computer user, who would probably be unaware that the file was on their machine.

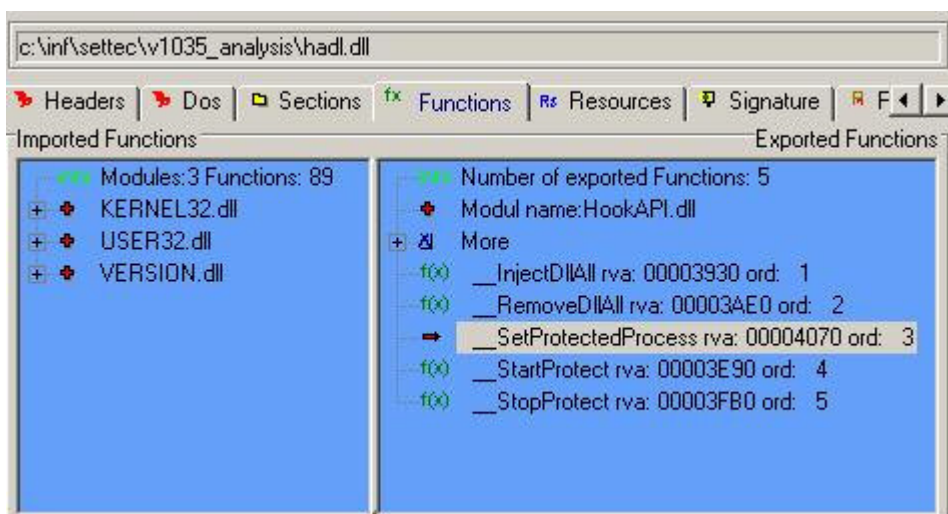
## The Protection Scheme

Once installed on the system, the Alpha-DVD program<sup>[3]</sup> creates the following registry subkey, which will run the protection program every time the machine starts:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run\”System  
Manager”=”%SYSTEM%\[RANDOM].EXE”
```

The use of random and obscure filenames in the %System% folder is a typical feature of malicious programs and is rarely seen in legitimate software. Fortunately, the Run registry subkey is not hidden, so users can search the registry, check for its presence, and eventually delete it. When the program is executed on Windows XP/2000 machines, it drops a copy of the 'HADL.DLL' library in the current directory. Using DLL injection techniques, it injects the library into every process that is currently running or that will run. The DLL is the core component of the protection software and it exports the following methods:

```
__InjectDllAll()  
__RemoveDllAll()  
__SetProtectedProcess()  
__StartProtect()  
__StopProtect()
```



**Figure 3:** The library HADL.DLL installed by Settec exports many public methods that can be accessed externally by any executable.

After the injection, the DLL uses system-hooking techniques to create a user-mode hook of the following APIs:

Hook no.	Library	Hooked API
1	KERNEL32.DLL	DeviceIoControl
2	KERNEL32.DLL	OpenProcess
3	NTDLL.DLL	NtCreateFile
4	NTDLL.DLL	NtQuerySystemInformation
5	WNASPI32.DLL	SendASPI32Command
6	ASAPI.DLL	SendASPI32Command
7	ELBYCDIO.DLL	ElbyCDIO_ExDoScsiIO
8	ELBYCDIO.DLL	ElbyCDIO_DoScsiIO

The goals of these hooks are completely different, so not all of them result in a rootkit. The rootkit part of the code is concentrated only in some of the hooks and there are some mitigating points that should be considered:

- The hooking is realized in user-mode using standard DLL injection, so this means that is easier to detect and remove.
- Many antivirus and security programs typically use a driver module for scanning, so they may be able to bypass the hooks.
- The DLL is not hiding files on the system.

The rootkit part of this module resides in the ‘NtQuerySystemInformation’ and ‘OpenProcess’ hooks, which were designed explicitly to hide a process from the Windows Task Manager and from any other standard process monitoring utilities.

The hook performed on ‘NtCreateFile’ does not hide files, but it prevents access to certain directories as part of the DVD protection strategy.

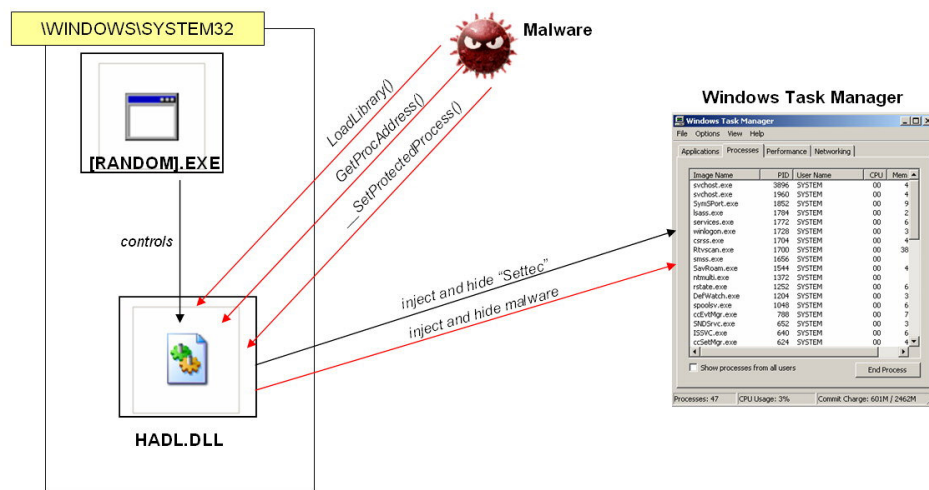
All the other hooks concern DVD/CD-ROM functions and may have an impact on system performance when reading or writing to DVD/CD discs. Finally, it should be mentioned that some of these hooks are designed to protect only Alpha-DVD protected discs, so these will not have any effect if a different DVD is inserted.

### What Are The Real Risks?

The protection design ‘as-is’ wasn’t intended to hide malicious code, but as happened in the story of HAL 9000, sometimes-good functionality can be used to do something completely different. The implementation of this protection is not safe because all the control logic resides in the .EXE file,

which utilizes the DLL component. Considered alone, HADL.DLL is a wide-open module that can provide all its functionality to any other process and executable. The diagram in Figure 4 shows one of the possible attack scenarios.

A malicious executable can check for the presence of HADL.DLL in the %Temp% or %System% folders, load it using LoadLibrary(), get the address of any exported function, and use it. Designing a program that uses HADL.DLL functions does not require advanced skills and needs only a few lines of code. For example, HADL.DLL will hide any process using its rootkit functionality if somebody calls the ‘\_\_SetProtectedProcess()’ method and passes a PID as parameter. Any programmer who has used a DLL library even once knows how to do that, and so this library represents a real security risk when it is installed on a computer.



**Figure 4:** Possible attack scenario where a malicious program exploits the HADL.DLL library using its system hooking capability.

A different type of risk is also present in the file-hooking code. As stated previously, the Alpha-DVD program is not hiding files, although it hooks ‘NtCreateFile’. This hook is necessary to prevent access to the \VIDEO\_TS and \AUDIO\_TS folders, where the encrypted .VOB files of movies are typically stored. This protection is controlled by the main executable and is activated only on DVD/CD-ROM drives, since the executable code contains a check routine for drive type using the Windows GetDriveType() function.

However it’s also possible to control HADL.DLL externally, by getting the address of the ‘\_\_StartProtect()’ function and by calling it using, for example, the ‘C’ drive as the parameter. In this second attack, a malicious program will be able to force the protection of the \VIDEO\_TS and \AUDIO\_TS directories of any drive, preventing access to every file contained in these folders. This means that if a malicious program activates the Settec protection on the C: drive and copies itself into one of these folders, the malicious file will be visible and listed by Explorer, but it will not be accessible, it won’t be able to be opened, and traditional antivirus programs will not be able to check it. Only security scanners that use a kernel mode driver, which can bypass HADL.DLL hooking, will be able to open the file for scanning.



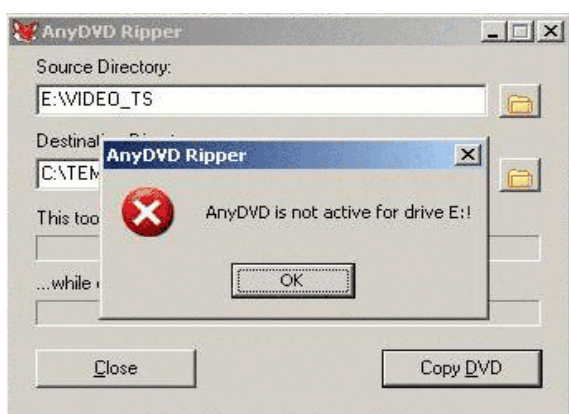
Finally, another attack scenario that exploits the file access protection of the Settec program can be realized if a malicious attacker creates a special CD-ROM disc that contains a malicious file inside the \VIDEO\_TS or \AUDIO\_TS folder. If this disc is created with characteristics (label, files on disc, structure, etc.) that make it similar to an original Alpha-DVD disc, the protection agent will automatically protect the malicious disc and prevent access to the mentioned folders.

## Competitive Antagonism In Legitimate Software

At the end of this story there is one more point that should be considered by the software industry and by developers. In the past, many variants of malware have contained aggressive code against other variants of malware. For example, the recent Trojan.Satiloler.E tries to terminate a long list of processes that include processes belonging to Trojan.Anserin, SpyAxe, Trojan.Abwiz, SpySheriff, and to some Backdoor.Nibu variants. Similarly, all the recent Beagle variants create mutexes to prevent NetSky worms from launching.

This phenomenon is not shocking if observed in a highly competitive environment like the world of malware, where nothing is either controlled or legal. But what if something similar started to happen between legitimate software programs?

Imagine Web-browsing software that, once installed, tried to disable certain features of FireFox or Internet Explorer for a competitive reason. I was very surprised when I realized the Alpha-DVD protection hooks in memory the code of 'ELBYCDIO.DLL', which is a legitimate library used by the CloneDVD and AnyDVD programs (see Figure 5). While these programs can be used for piracy, modifying such programs without clear notification and consent could be the start of a slippery slope.



**Figure 5:** As part of the protection strategy, when the Alpha-DVD agent is active some popular DVD ripping programs may not work correctly while accessing to the protected disc.

## Conclusions

Alpha-DVD DRM protection contains rootkit-like code that may allow other third party programs to hide their processes and prevents security software from having access to their files. This code can readily be used by malware authors with little or no knowledge of rootkit techniques.

Settec quickly released a free uninstaller for Alpha-DVD 1.0.3.5<sup>[4]</sup> and an updated version of the agent (1.0.4.0), which does not include the security issues discussed in this article. At the time of writing this article, few antivirus programs have added detection for this security risk.

## References

[1] Original post by German users complaining about the new protection system found on the Mr. & Mrs. Smith DVD

<http://forum.cinefacts.de/showthread.php?t=153246>

[2] Description of the Settec Alpha-DVD protection scheme

[http://www.settec.net/eng/pro\\_alphadvd.htm](http://www.settec.net/eng/pro_alphadvd.htm)

[3] Complete analysis of SecurityRisk.Settec

<http://securityresponse.symantec.com/avcenter/venc/data/securityrisk.settec.html>

[4] Settec uninstaller and security update for Alpha-DVD agent is available at:

<http://uninstall.settec.com/eng>

## About the Author

Elia Florio is a software engineer with the Symantec Security Response team, based in Dublin, Ireland. Elia graduated from the University of Calabria (UNICAL), Italy with a Bachelor of Computer Engineering in 2003. Elia previously worked for Value Partner and for Accenture on a variety of projects, including security-related consulting. Elia has written several articles for industry magazines and has contributed to a number of vulnerability announcements.



## **About Symantec**

Symantec is the global leader in information security, providing a broad range of software, appliances, and services designed to help individuals, small and mid-sized businesses, and large enterprises secure and manage their IT infrastructure.

Symantec's Norton™ brand of products is the worldwide leader in consumer security and problem-solving solutions.

Headquartered in Cupertino, California, Symantec has operations in 35 countries.

More information is available at [www.symantec.com](http://www.symantec.com).

Symantec has worldwide operations in 35 countries. For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 800 745 6054.

Symantec Corporation  
World Headquarters  
20330 Stevens Creek Boulevard  
Cupertino, CA 95014 USA  
408 517 8000  
800 721 3934  
[www.symantec.com](http://www.symantec.com)

Symantec and the Symantec logo are U.S. registered trademarks of Symantec Corporation. Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other brand and product names are trademarks of their respective holder(s). Any technical information that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation. NO WARRANTY. The technical information is being delivered to you as-is and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained herein is at the risk of the user. Copyright © 2006 Symantec Corporation. All rights reserved.  
04/05 10406630