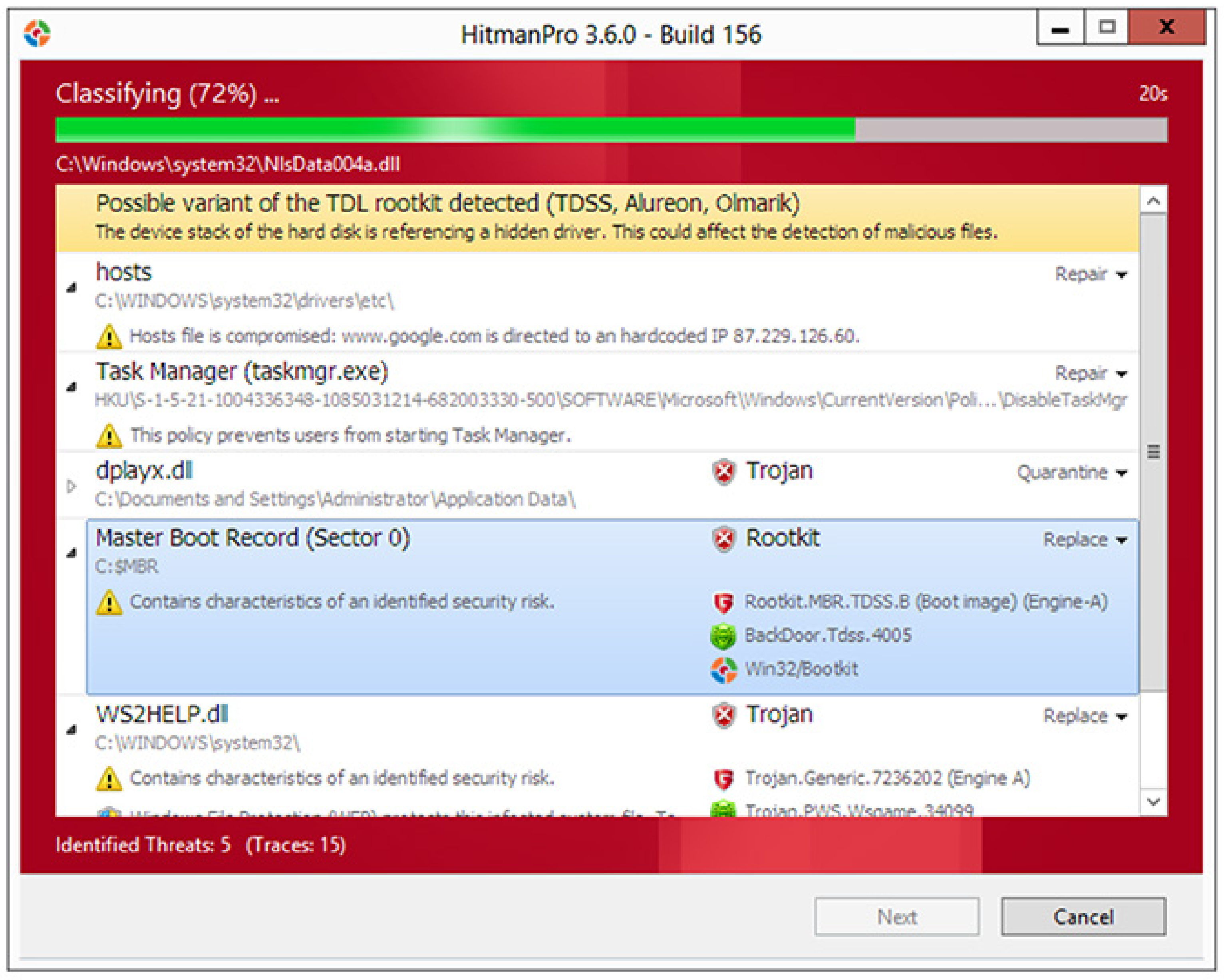
SurfRight

HitmanPro

Eliminates "zero day," deeply embedded and persistent threats that your antivirus software does not detect or remove.

Second Opinion

Today's malware is designed to bypass antivirus defenses and effectively hides from both security software and the computer user. Antivirus programs, blacklists and other security software that require prior knowledge of a threat are ineffective against "zero day" malware. Our real-world statistics – covering millions of scanned computers – show that 1 out of 3 computers have become infected despite real-time protection from up-to-date antivirus software.



Classifying (72%) ... 20s

C:\Windows\system32\NlsData004a.dll

Possible variant of the TDL rootkit detected (TDSS, Alureon, Olmarik)
The device stack of the hard disk is referencing a hidden driver. This could affect the detection of malicious files.

hosts
C:\WINDOWS\system32\drivers\etc\
Hosts file is compromised: www.google.com is directed to an hardcoded IP 87.229.126.60.

Task Manager (taskmgr.exe)
HKU\S-1-5-21-1004336348-1085031214-682003330-500\SOFTWARE\Microsoft\Windows\CurrentVersion\Poli...\DisableTaskMgr
This policy prevents users from starting Task Manager.

dplayx.dll — Trojan
C:\Documents and Settings\Administrator\Application Data\

Master Boot Record (Sector 0) — Rootkit
C:$MBR
Contains characteristics of an identified security risk.
Rootkit.MBR.TDSS.B (Boot image) (Engine-A)
BackDoor.Tdss.4005
Win32/Bootkit

WS2HELP.dll — Trojan
C:\WINDOWS\system32\
Contains characteristics of an identified security risk.
Trojan.Generic.7236202 (Engine A)
Trojan.PWS.Wsgame.34099

Identified Threats: 5 (Traces: 15)

HitmanPro reveals deeply embedded persistent threats in crtitical system objects

HitmanPro works alongside your existing antivirus program and is especially effective at detecting and removing "zero day" or other malware designed to evade detection by traditional antivirus software. It combines cloud computing, multi-criteria heuristics and behavioral analysis to effectively reveal and bypass the cloaking and deceiving techniques employed by modern malware.

HitmanPro is the only full spectrum antivirus program capable of both detecting and removing deeply embedded persistent threats, like ZeroAccess, TDL3, TDL4, Mebroot, Pihar, Cidox, as well as other malware that your antivirus software does not detect.

Cloud Assisted Miniport Hook Bypass

The toughest types of malware are rootkits. Rootkits embed themselves deep in the operating system where they hide from antivirus software. The longer a rootkit stays alive on a computer, the more profit the malware authors make because the computer is under their control.

Highly advanced rootkits, like TDL4 and Mebroot, work on both 32-bit and 64-bit versions of Windows and infect the Master Boot Record (MBR). These so called Bootkits start before Windows boots up, which gives the bootkit an obvious advantage. Any protection mechanism imposed by Windows (or antivirus program that is loaded by Windows) can be defeated – the program that is started first has control over the others.

Our proprietary Cloud Assisted Miniport Hook Bypass technology collects hard disk miniport driver information from clean computers and stores a representation of this information (a fingerprint of a few bytes) in the Cloud. When HitmanPro detects a hook on the hard disk driver, it consults the Cloud on how to work around it. This allows HitmanPro to bypass the rootkit's hooks and examine the actual infected sectors. This works for ANY hard disk driver and not just the common ones.

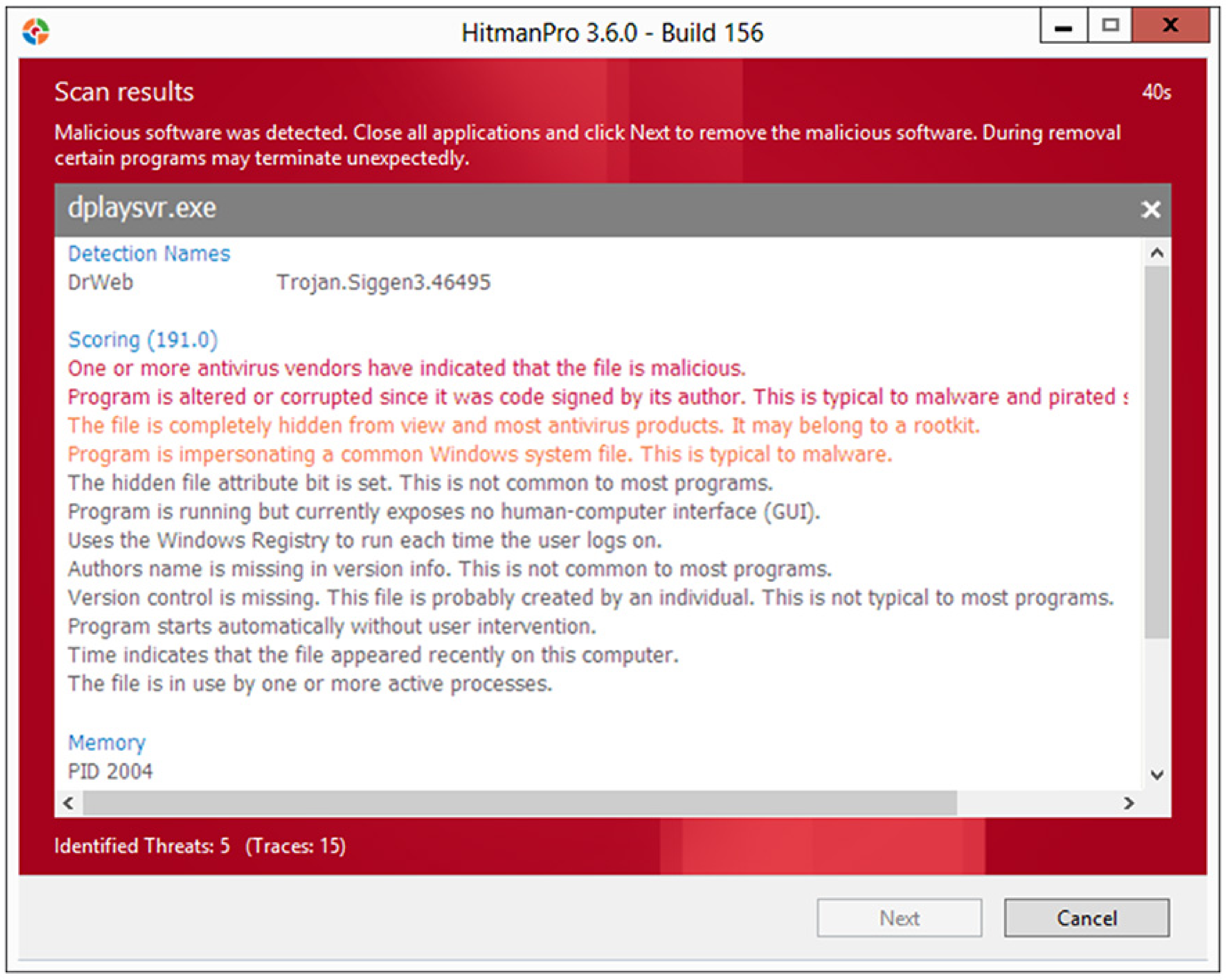
HitmanPro is a second opinion scanner, designed to rescue computers that have become infected with viruses, spyware, Trojans, rootkits and other threats, despite real-time protection from up-to-date antivirus software.

Behavioral Scan

Most traditional security software detects known malware by searching programs for code that matches a signature in the database. Malware authors evade this detection by simply creating new malware or malware variants. HitmanPro identifies malware with its Behavioral Scan, an intelligent malware detection system based on association mining. It identifies and correlates many behaviors and traits, and assigns each program and running binary a threat severity score. It gathers actionable intelligence by probing programs and binaries for structure anomalies, impersonation, tampering, visibility, activity, boot survivability, uninstall ability, reputation[1], its origin and relation to other memory, file and registry objects and their characteristics and reputations.

HitmanPro reveals binaries that act and look like malware.

HitmanPro does not require unique signatures (prior knowledge) of every malware sample or strain to detect malware – so no need to wait for your incumbent antivirus vendor to provide a detection signature.



Malicious software was detected. Close all applications and click Next to remove the malicious software. During removal certain programs may terminate unexpectedly.

dplaysvr.exe

Detection Names

DrWeb Trojan.Siggen3.46495

Scoring (191.0)

```
One or more antivirus vendors have indicated that the file is malicious.
Program is altered or corrupted since it was code signed by its author. This is typical to malware and pirated s
The file is completely hidden from view and most antivirus products. It may belong to a rootkit.
Program is impersonating a common Windows system file. This is typical to malware.
The hidden file attribute bit is set. This is not common to most programs.
Program is running but currently exposes no human-computer interface (GUI).
Uses the Windows Registry to run each time the user logs on.
Authors name is missing in version info. This is not common to most programs.
Version control is missing. This file is probably created by an individual. This is not typical to most programs.
Program starts automatically without user intervention.
Time indicates that the file appeared recently on this computer.
The file is in use by one or more active processes.
```

Memory

PID 2004

Identified Threats: 5 (Traces: 15)

HitmanPro reveals actionable intelligence in a human readable format

Threat Remediation

Today's resilient malware piggybacks on critical system files or boot records to subvert Windows and antivirus software, even before the operating system boots.

HitmanPro can remove persistent threats from within the running operating system and blocks malware reinfection attempts by protecting specific registry key and file locations. No need to reimage infected computers or physically access the computer to boot from a time consuming rescue disk.

No Installation

HitmanPro is a blazing fast on-demand scanner and does not need to be installed, contrary to most other security software. It can be started directly from USB Flash Drive, CD/DVD, hard disk or network attached storage. This is particularly useful in situations where malware prevents the installation of security software.

HitmanPro is always up-to-date and you don't have to download updates thanks to our proprietary cloud technology.

[1] Reputations are provided by our Scan Cloud infrastructure where also expertise from third parties like Bitdefender, Emsisoft, Ikarus, G Data and Dr.Web resides.

Includes extensive command-line interface and XML logging for scripting in a network environment.
Local installation requires 8 megabytes (MB) of hard disk space.
http://www.surfright.com/downloads/business

32- and 64-bit
Windows 7
Windows Vista
Windows XP
Windows Server 2008
Windows Server 2003

Compatible with Windows 7