

Anti-Malware



HitmanPro is a second opinion scanner designed to rescue computers that have become infected with viruses, spyware, Trojans, rootkits and other threats.

Today's malware is designed to bypass antivirus defenses and effectively hide 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 one out of three computers has become infected, despite real-time protection from up-to-date antivirus software.

HitmanPro works alongside your existing antivirus software to detect and remove zero-day and 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 deceptive techniques employed by modern malware.

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

How HitmanPro Integrates with LabTech

HitmanPro is integrated with the LabTech interface to enable centralized control of instant scan and remediation activities. Through the LabTech dashboard, partners can:

- Execute a scan
- Execute a clean
- Customize the schedule for automated scan and clean
- Create a support ticket when malware has infected a machine

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 the rootkit stays alive on a computer, the more profit the malware authors make because the computer is under their control. Highly advanced rootkits such as 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 by an antivirus program that is loaded by Windows) can be defeated, because the program that is started first has control over the others.

HitmanPro's 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.

Behavioral Scan

Most traditional security software detects known malware by searching programs for code that matches an existing signature in the database. Malware authors evade this detection by simply creating new malware or malware variants. HitmanPro does not need prior knowledge of every malware sample or strain to detect malware.

HitmanPro identifies malware with its Behavioral Scan, an intelligent malware detection system based on association mining that identifies and correlates many behaviors and traits, and assigns each program and running binary a threat severity score.

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 can block malware reinfection attempts by protecting specific registry key and file locations. There is no need to reimagine infected computers or physically access the computer to boot from a time consuming rescue disk.

No Installation

HitmanPro is a blazingly fast on-demand scanner and unlike most other security software, it does not need to be installed – it can be started directly from a 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 never have to download signature updates thanks to its proprietary cloud technology.

