Hitman Pro 3

Real-World Malware Statistics

October/November 2009
Table of Contents

Introduction to Hitman Pro .......................................................................................................................... 3
Extensive Virus Recognition .......................................................................................................................... 3
Behavioral Scan ............................................................................................................................................ 4
  Association Mining ..................................................................................................................................... 4
  Unobtrusive ................................................................................................................................................ 5
  Fast Scanning .............................................................................................................................................. 5
Scan Cloud .................................................................................................................................................... 6
  Striders ......................................................................................................................................................... 6
  Unknown Files ........................................................................................................................................... 6
Threat Confidence Levels ............................................................................................................................. 6
Malware Analyzer .......................................................................................................................................... 6
  Connecting the AV Industry ..................................................................................................................... 7
Crusader ........................................................................................................................................................ 8
Zero-day or Early Life Malware .................................................................................................................... 8
Infected despite AV Protection ....................................................................................................................... 8
Malware Removal Test .................................................................................................................................. 9
Real-World Statistics ................................................................................................................................... 10
  AMTSO ...................................................................................................................................................... 10
  AV Product Efficacy ................................................................................................................................. 10
    Licensed Technology .............................................................................................................................. 10
  Disclaimer ................................................................................................................................................ 11
  False positives .......................................................................................................................................... 11
Computer Infection Overview ..................................................................................................................... 12
Infected Windows Versions ........................................................................................................................... 12
  Windows 32-bit (x86) ............................................................................................................................... 12
  Windows 64-bit (x64) .............................................................................................................................. 12
Top 20 Detected Malware ............................................................................................................................. 13
  Malware Defeating AV Products ............................................................................................................ 14
  Generics ..................................................................................................................................................... 14
  Scan Cloud Effectiveness ......................................................................................................................... 14
AV Product Infection Ratios .......................................................................................................................... 14
  Least infected ............................................................................................................................................ 15
  Most infected ........................................................................................................................................... 15
Detection and Removal of Live Infections ..................................................................................................... 16
  TDSS/Alureon Rootkit .............................................................................................................................. 16
Conclusions ................................................................................................................................................... 17
Introduction to Hitman Pro

Hitman Pro 3 is a solution to counter malicious software such as viruses, spyware, Trojans, worms, adware, bots and rootkits, also known as malware (malicious software). Hitman Pro 3 catches more new malware than traditional virus scanners thanks to new innovative technology which also has a much shorter scan time than traditional Anti-Virus (AV) software. Hitman Pro 3 is an on demand scanner without a real-time component and can be run directly from a USB flash drive, CD/DVD, local or network attached hard drive. This, plus the short scan time, makes Hitman Pro 3 an ideal second opinion AV scanner.

Extensive Virus Recognition

Traditional AV software depends on the quality of the virus signatures and in some cases on the heuristic capabilities of the AV program. SurfRight partners with 5 suppliers of security software and has access to 7 different antivirus engines and databases. Despite the tremendous effort of AV companies, relying on just one Security Suite or Anti-Virus program is no longer adequate against today’s malware and this report will give this statement foundation.

Many researchers have come to the same conclusion.

**Prevx**
“Every day, popular security products are missing thousands of infections” ¹

**Cyveillance**
“Even the most popular AV solutions detect less than half of the latest malware threats.” ²

**Damballa**
“This is due in part to the fact that enterprise-grade antivirus and IDS/IPS fail to capture 20% to 70% of new threats, including targeted attacks and common Trojan attacks” ³

**FireEye**
“So the conclusion is that AV works better and better on old stuff” ⁴

**Ikarus**
“The increasingly huge number of new malware samples challenges every analysis team. An in-depth analysis performed by human experts may take several days and uses valuable human resources.” ⁵

**VB100**
“A few renowned anti virus programs do not pass the VB100 test.” ⁶

For Hitman Pro 3 SurfRight developed the Behavioral Scan, the Scan Cloud (containing multiple AV technologies) and the Crusader, to locate, identify and remove known and unknown malware. It does this in just a few minutes and without installing any software on the computer of the end user.

---

¹ http://www.prevx.com
⁵ http://www.virusbtn.com/conference/vb2009/abstracts/Mandl.xml
⁶ http://www.virusbtn.com/vb100/index
Behavioral Scan

Hitman Pro 3 is an on-demand signature-less behavioral and cloud based malware scanner. The behavioral based scanner generates a threat score for each file it finds. Depending on this threat score it sends files that are potentially malicious to our Scan Cloud for instantaneous in-depth scanning and verification (which uses our own and multiple technologies from our antivirus partners for virus naming). The Scan Cloud returns the scan results within seconds and the verified malicious files are removed from the computer.

Association Mining

The model behind the Behavioral Scan is an intelligent PE-malware detection system based on association mining and is designed to distinguish legitimate from malicious software. It does not contain signatures to detect malicious software. Instead, it tries to determine: (incomplete list)

Dynamic
- where a file comes from
- how it got on the system
- whether it can be uninstalled appropriately
- how it (automatically) starts and if it is currently running in memory
- if it is visible for the user and through Windows API's
- if it is communicating with untrustworthy computers on the Internet
- if it is associated with another (likely or verified malicious) file on the system
- what people say about the file (program) on security related websites (our Gossip Rating system)
- its global threat confidence level (reputation)

Static
- if the file is a known threat
- which publisher created it
- whether or not it is digitally signed with a trusted (non stolen) certificate
- if it’s compressed or encrypted / obfuscated to thwart virus research
- if it has anomalies commonly found in malicious software (PE analysis)

Potential malicious software is sent to the Scan Cloud for verification and virus naming while legitimate software is not queued for upload or further analysis.
Unobtrusive

Contrary to behavioral blockers, the design of the Behavioral Scan is an unobtrusive observation of computer activity. Hitman Pro 3:

- does not require user interaction
- does not need to run continuously
- does not hook into Windows APIs

The Behavioral Scan also collects information on related registry keys, files and shortcuts to ensure complete removal by Hitman Pro’s malware removal engine Crusader (which we designed to cope with the most resilient threats).

Fast Scanning

Hitman Pro 3 scans faster than traditional AV programs because it has some different approaches:

- The Behavioral Scan determines which files are safe and which are probably not, depending on their actions. This means not every file needs to be scanned extensively.

- With the built-in whitelist the Behavioral Scan skips known safe files after a quick analysis. The whitelist contains hashes and signatures of known safe Windows 2000, XP, 2003, Vista, 2008 and Windows 7 system files.

- The disk scanner of the Behavioral Scan is not affected by disk fragmentation. Instead of working through folders and files alphabetically (like a human), it scans files in the order they are physically stored and encountered on the disk. Practically, this means that Hitman Pro directs the read head of a regular hard disk to move in just one direction across the disk platter – optimizing the speed of reading data – instead of causing the reading head to move back and forth like a regular AV program, which causes delay.

- The Behavioral Scan is multithreaded (to efficiently use the capabilities of the CPU hardware). Hitman Pro 3 will perform disk, registry, network (for example cloud scanning) and internal analysis tasks simultaneously.

- Hitman Pro will only scan files with a so called PE-header, which are currently loaded in memory, start automatically or have a shortcut. It does not scan or upload any documents to the Scan Cloud which guarantees privacy.
Scan Cloud

Cloud computing is the use of computer technology using the Internet (the term cloud is a metaphor for the Internet). Cloud-based Hitman Pro 3 handles in-depth scanning of files on a remote server, rather than on a user’s machine. The Scan Cloud of Hitman Pro 3 contains knowledge and intelligence of multiple collectives and AV technologies from several AV partners. This significantly differs from other currently available cloud-based AV products who are only using their own research and technology.

Striders

The Scan Cloud for Hitman Pro 3 is a group of computers (Striders) connected to the Internet. Each Strider contains multiple (signature based) AV products from our trusted partners to quickly scan if a file is indeed malicious.

The efficient design of the Behavioral Scan and the extensive research behind it ensures that on a typical Windows Vista workstation (about 400,000 files) only a handful of files (the potentially malicious ones) need to be uploaded to and scanned by the Scan Cloud for verification and virus naming. Only suspicious PE-files are sent to the Scan Cloud. Every upload is anonymous and by default encrypted.

Unknown Files

The Scan Cloud identifies tens of thousands of new threats on a daily basis. But despite the amount of recognition technology from our collaboration with 5 AV suppliers, the Scan Cloud is often unable to identify so called zero-day or early life malware. In this case end users can use Early Warning Scoring (EWS) in Hitman Pro 3 to reveal the active yet unknown potential malicious files.

Threat Confidence Levels

The Scan Cloud receives threat score information on each file it receives, anonymously. By correlating information between multiple users the Scan Cloud generates so called Threat Confidence Levels (or reputations) which can be used to counter zero-day or early life malware.

The Scan Cloud contains global information on:

- which malware is currently infecting computers
- which malware is capable of bypassing certain AV protected computers
- which yet unknown files are interesting for immediate human analysis
- which web sites are hosting malware

Malware Analyzer

By centrally correlating the threat information generated by Hitman Pro 3, the Scan Cloud can be used to identify new threats on a global scale. The Behavioral Scan in Hitman Pro 3 has turned every system into an in-depth malware analyzer.
Connecting the AV Industry

The Scan Cloud is also capable of exchanging malware files and other threat information with our AV partners – something major players in the AV industry are still dreaming about.\(^7\)

\(^7\) http://www.virusbtn.com/conference/vb2009/abstracts/LastMinute5.xml
Crusader

Besides the Behavioral Scan and the Scan Cloud we also created a universal malware removal engine to handle infected and resilient malicious files. We named our engine Crusader and it is capable of not only handling malicious files, related registry keys and shortcuts but is also responsible for replacing essential but infected Windows files with safe versions (so Windows remains running stable).

Also, the Crusader will kill malicious files in memory and literally disables them on the disk, practically killing the files. Remaining objects are cleaned during boot by Crusader’s native NT bootdeleter which runs before other programs start and the desktop appears.

Zero-day or Early Life Malware

The infection ratio statistics in this paper are based on these malicious files received by our Scan Cloud. End users download and run Hitman Pro 3 when they expect an infection or want a second opinion (e.g. after their antivirus software found an infection on the computer). This means that the numbers in our statistics generally represent the malware currently infecting computers, so called zero-day or early life malware. "Old" malware that has been around for some time was probably detected and removed by the existing AV program on the computer and will therefore not be found and uploaded by the Behavioral Scan.

Infected despite AV Protection

Hitman Pro 3 also checks which AV software is used on the computer. Their names are send to the Scan Cloud if the detected AV software is up-to-date (healthy) and has on-access scanner enabled. As a result, the Scan Cloud knows which AV programs are currently unaware of (or unable to remove) a particular threat. For example, Hitman Pro 3 often finds (variants of) the TDSS rootkit on AV protected systems. This rootkit deploys advanced cloaking techniques that causes severe problems for modern AV products and can even defeat them completely. Testing AV products using an on-demand scan to identify inactive samples is therefore a somewhat unfair test since the scanned malware is not allowed to deploy or use its defensive weaponry to stay alive. Contrary to traditional AV products Hitman Pro 3 is especially designed to battle live malware and to detect its stealth weaponry.
Malware Removal Test

The organization AV-Comparatives performs independent tests of antivirus software. Every three months they perform “on-demand” and “retrospective/proactive” detection rate tests. Recently they published their first test report that focuses on the malware removal/cleaning capabilities of AV products. Their results are also quite staggering. AV products detecting over 99% in AV-Comparatives on-demand tests, score poorly once malware is able to infect the system. And this test was performed under laboratory conditions using known and widespread malware samples.

Real-World Statistics

Where tests from independent organizations are performed under closed laboratory conditions (using malware samples from months or even years ago), this report is based on malicious software found by Hitman Pro 3 on actually infected computers, encountered in the real world.

AMTSO

With respect to the Anti-Malware Testing Standards Organization (AMTSO), these statistics are not based on any laboratory tests. These statistics are derived from the field, based on PCs that are really infected with active malware (live threats). So these statistics are a realistic representation of an AV product efficacy because the (dynamic) malware information is collected from victim machines. This also means that the statistics are conform AMTSOs’ quality and quantity criteria on functionality, diversity, relevance and freshness.

AV Product Efficacy

As mentioned earlier, Hitman Pro 3 also collects information about the AV program responsible for (on-access) virus protection on the scanned machine. When Hitman Pro 3 found malware, it does not necessary mean that the installed AV product is unaware of this threat. It could also mean that this AV program was technically unable to read, remove or disinfect the infected file because of effective rootkit-like cloaking or hooking techniques.

Good examples are new TDSS/Alureon rootkit variants. Ex. Hitman Pro 3 scans, finds, reads and sends the main TDSS/Alureon driver file to the Scan Cloud where renowned AV products from our partners (also) identify it as malicious. But when you would use the AV product itself (instead of Hitman Pro) on the infected system, it is unable to detect or remove the rootkit. For a separate (laboratory) test, see page 13.

Licensed Technology

Some AV vendors have licensed security technology from other vendors. For example, BullGuard licensed the BitDefender AV engine. Also PC Tools, F-Secure and G Data licensed multiple technologies from other vendors. But incorporating technologies from other vendors does not automatically mean the end-product is superior. For example, being able to identify a malicious file with a licensed AV engine does not automatically mean an AV product is also capable of accessing or removing this file from an infected system. As indicated earlier, scan and malware removal technology is just as important as a rich AV engine.

9 http://amtso.org/amtso---download---amtso-best-practices-for-dynamic-testing.html
Disclaimer

Please keep in mind that the provided statistics do not represent any AV product efficacies, because there is a big difference in the amount of security layers software can provide. For example, AVG also provides LinkScanner which helps against drive-by-download infections. In addition Hitman Pro 3 does not take into account what other security measures are installed on the scanned computers, like additional spam filtering and firewall software, UAC settings, installed Windows updates, etc. The default web browser or version level of Adobe Reader, Flash, Java or Internet Explorer could also influence the protection level of a system. For example, the new Smart Screen Filter in Internet Explorer 8 offers much better protection against internet borne threats than Internet Explorer 7.

Please note that in our test group we see a lot more computers running an AV product from (for example) AVG, ALWIL and Avira than e.g. ESET and Kaspersky, because AVG, ALWIL and Avira offer a free version of their antivirus software.

False positives

A false positive, also known as a false detection or false alarm, occurs when an AV program detects a known virus string in an uninfected file. The file, while not infected with an actual virus, does contain a string of character that matches a string from an actual virus. A false positive can also occur when a program performs an action, which appears to the AV program to be a virus-like activity.

The Behavioral Scan in Hitman Pro 3 is also designed to look for virus-like activity and properties in files. And the Scan Cloud contains multiple AV programs to detect virus strings in the potentially malicious files received from Hitman Pro 3. Having multiple detection systems can increase the chance of false positives.

But, Hitman Pro 3’s systems work in tandem: a file must first have virus-like activity or properties before it is sent to the Scan Cloud to scan it for known virus strings. To further reduce the chance of false positives the entire system contains two whitelists. One is built into the Hitman Pro 3 client application and the other resides in the Scan Cloud. Also 2 of our AV partners in the Scan Cloud are able to detect legitimate files. In addition, only when a majority of renowned AV vendors in the Scan Cloud classify a file as malicious it is returned as such to the client application. When desired, the end-user can always change the default action associated with the final classification.

The statistics in this report are based on malicious files identified by at least 2 (or more) renowned AV vendors in our Scan Cloud.
Computer Infection Overview

For this real world statistics we monitored over 100,000 new users running Hitman Pro 3 during the period from October 10 to December 4, 2009 (55 days).

<table>
<thead>
<tr>
<th>Computers Total</th>
<th>Infected</th>
<th>Clean</th>
<th>With up-to-date AV</th>
<th>Without up-to-date AV</th>
<th>Infected with AV</th>
<th>Infected without AV</th>
</tr>
</thead>
<tbody>
<tr>
<td>107435</td>
<td>37898 (35%)</td>
<td>69537 (65%)</td>
<td>78828 (73%)</td>
<td>28607 (27%)</td>
<td>25038 (32%)</td>
<td>13002 (46%)</td>
</tr>
</tbody>
</table>

Looking at the table above, 32% of the computers protected by AV products are infected, despite the protective layer. And the difference between no virus protection and a real-time AV product is 14%.

Infected Windows Versions

The following two lists are overviews of the infected Windows operating systems our Hitman Pro 3 software encountered. The threshold for inclusion in these 2 overviews was 50 or more different infected computers. These percentages reveal that installing the latest Service Pack result in a security advantage.

Windows 32-bit (x86)

<table>
<thead>
<tr>
<th>Version</th>
<th>Infected %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 2000 Service Pack 4</td>
<td>32%</td>
</tr>
<tr>
<td>Windows XP RTM</td>
<td>52%</td>
</tr>
<tr>
<td>Windows XP Service Pack 1</td>
<td>46%</td>
</tr>
<tr>
<td>Windows XP Service Pack 2</td>
<td>45%</td>
</tr>
<tr>
<td>Windows XP Service Pack 3</td>
<td>34%</td>
</tr>
<tr>
<td>Windows Vista RTM</td>
<td>35%</td>
</tr>
<tr>
<td>Windows Vista Service Pack 1</td>
<td>31%</td>
</tr>
<tr>
<td>Windows Vista Service Pack 2</td>
<td>23%</td>
</tr>
<tr>
<td>Windows 7 RTM</td>
<td>33%</td>
</tr>
</tbody>
</table>

Windows 64-bit (x64)

<table>
<thead>
<tr>
<th>Version</th>
<th>Infected %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows XP Professional Service Pack 2</td>
<td>33%</td>
</tr>
<tr>
<td>Windows Vista Service Pack 1</td>
<td>25%</td>
</tr>
<tr>
<td>Windows Vista Service Pack 2</td>
<td>22%</td>
</tr>
<tr>
<td>Windows 7 RTM</td>
<td>24%</td>
</tr>
</tbody>
</table>
Top 20 Detected Malware

The table list below is a top 20 of malware that Hitman Pro 3 encountered during the period of October 10 to December 4, 2009 (55 days).

<table>
<thead>
<tr>
<th>Position</th>
<th>Malware Name</th>
<th>Infected Computers</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Generic</td>
<td>34845</td>
</tr>
<tr>
<td>2</td>
<td>FakeAV</td>
<td>13050</td>
</tr>
<tr>
<td>3</td>
<td>TDSS/Alureon</td>
<td>5915</td>
</tr>
<tr>
<td>4</td>
<td>Delf</td>
<td>4116</td>
</tr>
<tr>
<td>5</td>
<td>Virut</td>
<td>2868</td>
</tr>
<tr>
<td>6</td>
<td>Vundo</td>
<td>2421</td>
</tr>
<tr>
<td>7</td>
<td>Small</td>
<td>2342</td>
</tr>
<tr>
<td>8</td>
<td>OneStep</td>
<td>2093</td>
</tr>
<tr>
<td>9</td>
<td>OnLineGames</td>
<td>1946</td>
</tr>
<tr>
<td>10</td>
<td>Swizzor</td>
<td>1854</td>
</tr>
<tr>
<td>11</td>
<td>Cutwail</td>
<td>1792</td>
</tr>
<tr>
<td>12</td>
<td>Palevo</td>
<td>1690</td>
</tr>
<tr>
<td>13</td>
<td>Zbot</td>
<td>1584</td>
</tr>
<tr>
<td>14</td>
<td>Autorun</td>
<td>1577</td>
</tr>
<tr>
<td>15</td>
<td>Zlob</td>
<td>1368</td>
</tr>
<tr>
<td>16</td>
<td>Rustock</td>
<td>1251</td>
</tr>
<tr>
<td>17</td>
<td>Buzus</td>
<td>1236</td>
</tr>
<tr>
<td>18</td>
<td>Hilot</td>
<td>1154</td>
</tr>
<tr>
<td>19</td>
<td>Bredolab</td>
<td>1144</td>
</tr>
<tr>
<td>20</td>
<td>Vilsel</td>
<td>944</td>
</tr>
</tbody>
</table>

The Generic group contains all kinds of different malware and is not one particular infection. FakeAV is a group that consists of all kinds of rogue antivirus/antispyware software.
Malware Defeating AV Products

Hitman Pro 3 is designed as a second opinion scanner to battle live malware on AV protected computers. The majority of our end users run on-access AV protection on their computers so the malware detected by Hitman Pro 3 can be considered infections that are able to bypass, successfully hide from or are deliberately not detected by popular AV products. Probable causes:

1. All kinds of cloaking technology deployed by malware (rootkit behavior).
2. Polymorphic malware – changing packer/encryption (obfuscation) schemes per period or victim to defeat simple hash based signature detection in traditional AV products.
3. Polymorphic file infector viruses (like Virut) – these viruses add themselves to legitimate (system) files and requires special disinfection technology that most AV products lack.
4. Load, priorities and efficiency of malware research and response teams at AV vendors – these teams are responsible for catching and analyzing new threats, as well as signature creation to battle these.

Generics

The number one infection is a generic classification of a malicious file. This means AV vendors are trailing behind cybercriminals. The reason for this is that it often takes days (or even weeks) before AV vendors are aware of a new threat: a sample first needs to be captured and analyzed before researchers can develop and distribute a good signature to detect and remove this threat. These tasks take time.

To help customers proactively AV vendors often create several generic, often heuristics based, signatures to capture new variants or certain code sequences commonly found in known malware.

Heuristic generic classification is subject to some criticism. In comparisons it is not valid to count a generic malware classification. In the real-world, generic classifications prove to be very useful. Our statistics show that 80% of the generic malware classifications were made by 2 or more renowned AV vendors in our Scan Cloud.

Scan Cloud Effectiveness

The multiple AV technologies and products from different renowned AV vendors in our Scan Cloud are very successful in identifying the suspicious malware files intelligently picked by the Behavioral Scan in Hitman Pro 3.

A random test using data from November 23, 2009, shows that 42% of the new suspicious files on that day were identified as malicious by just 1 renowned AV vendor in our Scan Cloud. Rescanning the exact same files 2 weeks later (on December 7, 2009) resulted that only 8% remained identified by 1 AV vendor – all other files received a malware classification from 2 or more renowned AV vendors.
AV Product Infection Ratios

The Scan Cloud contains statistics about the on-access and up-to-date AV products that failed to detect or remove malware from infected computers. With these statistics we can generate an overview with least and most ‘infected AV products’. We do not publish this overview to the general public since it is not meant to discredit AV vendors. We create this overview to inform AV vendors. For the public we do provide details about the least and most infected AV product:

Please take the information provided in the Disclaimer (page 10) into account while interpreting these figures.

Least infected

The ‘least infected major AV product’ scored 15%. This figure indicates that Hitman Pro 3 found malware on 15% of the computers that were running this particular AV product (which could be considered the best AV product).

Most infected

39% of the computers running the ‘most infected major AV product’ were infected despite the protection that customers expect from their AV product. Note that over 8% of all scanned computers were running this particular AV product.
Detection and Removal of Live Infections

TDSS/Alureon Rootkit

The TDSS rootkit is in the malware top that Hitman Pro 3 detected during the period of October 10 to December 4, 2009 (55 days). With the release of the first Hitman Pro 3 last year, we also received the first sample of TDSS/Alureon rootkit from a victim’s machine in our Scan Cloud on October 30, 2008. More than one year later, this particular rootkit sample still beats almost every major AV product. Mentioned below a short list of current AV products that we have tested to determine if it would detect and remove a live TDSS/Alureon rootkit infection from October last year:

<table>
<thead>
<tr>
<th>AV Product</th>
<th>Able to detect infection</th>
<th>Able to remove infection</th>
</tr>
</thead>
<tbody>
<tr>
<td>a-squared Anti-Malware 4.5</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>AVG Anti-Virus 9.0</td>
<td>Yes&lt;sup&gt;10&lt;/sup&gt;</td>
<td>Yes</td>
</tr>
<tr>
<td>Avira AntiVir Premium 9</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>ESET NOD32 Antivirus 4</td>
<td>Yes, memory only&lt;sup&gt;11&lt;/sup&gt;</td>
<td>No</td>
</tr>
<tr>
<td>F-Secure Anti-Virus 2010</td>
<td>Yes</td>
<td>Yes&lt;sup&gt;12&lt;/sup&gt;</td>
</tr>
<tr>
<td>G Data Antivirus 2010</td>
<td>Yes, tmp files on disk only&lt;sup&gt;13&lt;/sup&gt;</td>
<td>No</td>
</tr>
<tr>
<td>Kaspersky Anti-Virus 2010</td>
<td>Yes, memory only&lt;sup&gt;14&lt;/sup&gt;</td>
<td>No</td>
</tr>
<tr>
<td>McAfee VirusScan Plus 13.15</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Panda Cloud Antivirus 1.0</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Prevx 3.0</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Symantec Norton AntiVirus 2010</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Trend Micro Internet Security 2010</td>
<td>Yes</td>
<td>No&lt;sup&gt;15&lt;/sup&gt;</td>
</tr>
</tbody>
</table>

Note: All tested AV products were fully-functional, had a proper Internet connection, running with up-to-date signatures and with default settings. Every scan was a full system scan. The test computer was running Windows XP Professional.

---

<sup>10</sup> Only detected after separate AVG Anti-Rootkit scan (not part of full system scan)

<sup>11</sup> No rootkit files found on disk

<sup>12</sup> Some traces remain

<sup>13</sup> Not able to detect rootkit driver file on disk and in memory

<sup>14</sup> Error reading the rootkit driver file on disk

<sup>15</sup> Trend Micro Internet Security says it is an untreatable virus
Conclusions

Numerous AV product tests appear every year and each claim a different winner. This fact alone should make you aware that there is no such thing as the best antivirus software.

Also, testing AV products using an on-demand scan to identify inactive malware samples is an unfair test: the scanned malware is not allowed to deploy or use its defensive weaponry to stay alive. The rather huge amount of infections that Hitman Pro 3 encounters on AV protected computers is a testimony to this fact.

Stealth technology is common in malware. And for this reason alone we advise everybody to not simply prolong a subscription for your AV product but to buy and install the latest version when it is time to re-subscribe. Older versions of AV products are often not equipped to handle the latest sophisticated threats that appeared this year. New versions often include new technologies to battle malware. Another advantage is that new versions of AV products are often largely redesigned to use less system resources than older versions.

Do not rely on just one protective layer to defend your data and privacy. Install a proper spam filter, update your web browser and make sure you have enabled the firewall on your computer or router. As the statistics in the report show (page 12), always install the latest Service Pack: computers running the latest Service Pack have a security advantage (are less infected). Also install the latest software updates and keep your AV product up-to-date. And ideally, periodically run a second opinion scan with one or more alternative AV software.