SurfRight
internet security engineers

Productbeschrijving

Hitman Pro 3.5

Inhoudsopgave

Wat is Hitman Pro 3

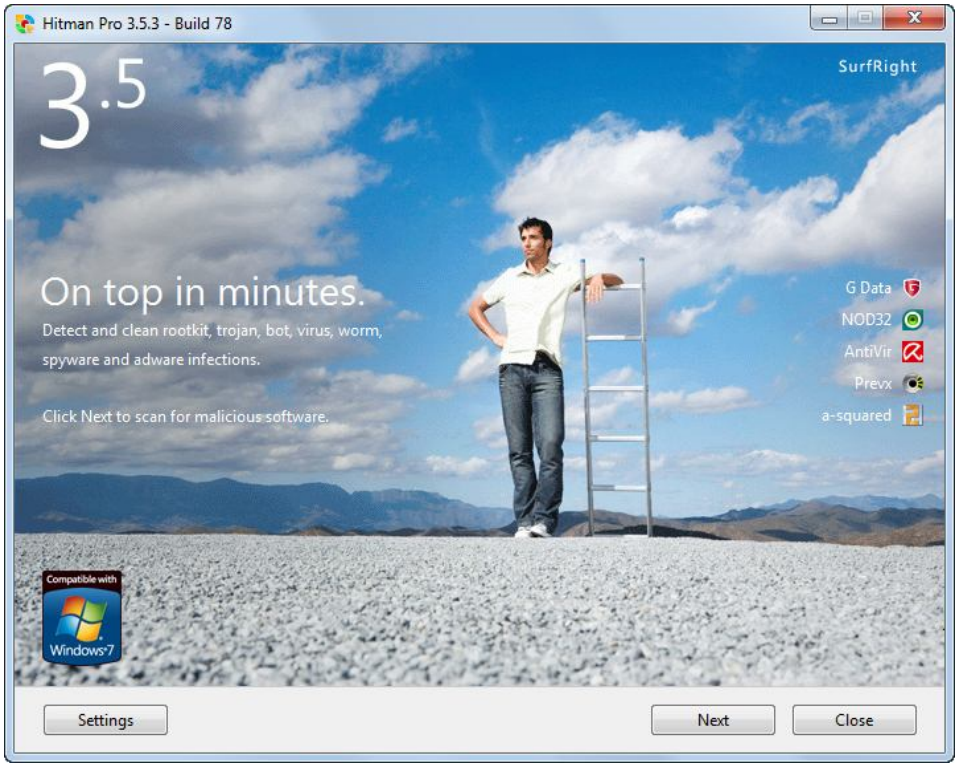
Hitman Pro 3 is een programma tegen schadelijke software, zoals virussen, spyware, Trojaanse paarden, wormen, adware, bots en rootkits – gezamenlijk ook bekend als malware (**mal**icious soft**ware**). Dankzij nieuwe technologie vangt Hitman Pro 3 veel meer nieuwe malware dan traditionele virusscanners. Het heeft daarbij ook een veel hogere scansnelheid dan gebruikers gewend zijn van antivirussoftware.

Hitman Pro 3 is ontworpen om bestaande actuele bedreigingen te verwijderen die (nog) niet door de bestaande antivirussoftware is herkend.

Hitman Pro 3 biedt geen doorlopende bescherming. We adviseren daarom ook om Hitman Pro naast traditionele antivirussoftware te gebruiken. Omdat het scannen met Hitman Pro over het algemeen slechts een paar minuten duurt, is het voor de gebruiker niet bezwaarlijk om de PC regelmatig (dagelijks of zelfs vaker) door Hitman Pro te laten controleren.

In dit document worden de achtergronden en innovatieve technieken besproken die Hitman Pro 3 zo bijzonder maken.

Screenshot



Zeer rijke virusherkenning

Een antivirusprogramma is zo goed als de virusdefinities (en eventuele heuristische capaciteiten) van dit programma. Doordat SurfRight B.V. samenwerkt met 5 fabrikanten van beveiligingssoftware heeft Hitman Pro 3 de beschikking over niet 1 of 2 maar 7 verschillende antivirusengines en databases.

7 antivirusengines

Elke dag verschijnen tienduizenden nieuwe malware exemplaren en varianten en elke antivirusfabrikant heeft zijn eigen virusonderzoekers en technische mogelijkheden om deze nieuwe bedreigingen te ontdekken, te onderzoeken en te definiëren. Gezien de moeite die criminelen doen om hun malware zo lang mogelijk (liefst onzichtbaar) op computers te houden, de relatief geringe onderzoekscapaciteit van beveiligers en de enorme hoeveelheid nieuwe malware dat dagelijks verschijnt is 1 antivirusprogramma nooit direct opgewassen tegen alle malware die rondgaat, hoe goed het netwerk, de onderzoekers, technologie (en marketing) van de fabrikant ook is.

Ondanks virusbescherming raakt het merendeel van de computers toch geïnfecteerd. We zien dit niet als enige, andere beveiligers zien dit ook:

Prevx "Every day, popular security products are missing thousands of infections"
www.prevx.com

Cyveilance "Even the most popular AV solutions detect less than half of the latest malware threats."
http://www.cyveillance.com/web/docs/WP_CyberIntel_H1_2009.pdf

VB100 http://www.virusbtn.com/vb100/index

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"
http://www.damballa.com/downloads/press/Failsafe_3_(PR_FINAL_2009-3-2).pdf

FireEye "So the conclusion is that AV works better and better on old stuff"
http://blog.fireeye.com/research/2008/11/does-antivirus-stop-bots.html

Het hebben van meerdere antivirusengines in combinatie met nieuwe innovatieve technieken is dus bittere noodzaak om zo snel en zoveel mogelijk bedreigingen te kunnen identificeren.

Dagelijks scannen

Antivirussoftware zou alle bedreigingen moeten tegenhouden zodra of voordat het de PC op komt. Maar fabrikanten van antivirussoftware weten ook dat ondanks alle moeite toch bedreigingen langs de beveiligingssoftware komt. Daarom wordt de antivirussoftware standaard altijd zo ingesteld dat het de computer dagelijks scant, zodat het toch de bedreigingen kan verwijderen die het eerder nog niet direct kende (en dus niet tegenhield, met alle gevolgen van dien).

Hitman Pro 3 is overigens ook standaard ingesteld om dagelijks (bij aanmelding) de computer te controleren op schadelijke software.

Gedragsscan

De methodiek die de bekende antivirusfabrikanten gebruiken (zie 7 antivirusengines, pagina 5) maakt duidelijk dat er een oneindig kat-en-muisspel gaande is: beveiligers lopen continu hard achter de cybercriminelen aan om hun klanten op tijd te kunnen beschermen.

Om niet ook in dit kat-en-muisspel te belanden heeft SurfRight voor de ontwikkeling van Hitman Pro 3 ruim 300.000 virusexemplaren op virusactiviteit onderzocht, met als doel deze op uniforme wijze te kunnen ontleden, zodat we precies inzicht hebben in de kenmerkende eigenschappen van malware. Daarnaast hebben we nog 2 eisen opgesteld: het scanproces moet binnen 5 minuten zijn afgerond en de gebruiker mag niet om hulp worden gevraagd - Hitman Pro 3 is bedoeld voor mensen die geen affiniteit met computerbeveiliging hebben of geen moeilijke vragen kunnen beantwoorden. Uit dit technisch onderzoek is een zeer uitgebreid model ontstaan. Dit unieke en innovatieve model hebben wij de Gedragsscan genoemd en is sinds de beschikbaarheid van Hitman Pro 3 in november 2008 nog steeds effectief tegen alle actuele bedreigingen.

Hitman Pro 3 scant een computer op virusactiviteit en verdachte bestanden en weet op een systeem met ruim 400.000 bestanden (bijvoorbeeld Windows Vista) binnen 2 minuten precies de mogelijke gevaren te detecteren – slechts een handvol bestanden hoeven dan nog maar door onze partners geïdentificeerd (gescand) te worden. Om deze bestanden te identificeren plaatsen we de antivirussoftware van onze partners niet meer op de computer van de eindgebruiker (ruim 250 megabytes aan noodzakelijke bestanden) maar hebben we de Scanwolk ontwikkelt.

In luttele seconden worden de meeste bestanden direct geïdentificeerd door de Scanwolk. Het is echter ook heel goed mogelijk dat één of meerdere bestanden ongeïdentificeerd blijven. In dat geval biedt de door Hitman Pro verzamelde informatie en het scoresysteem van de Gedragsscan uitkomst. Hiermee kunnen gebruikers onbekende verdachte bestanden (zogenaamde “zero-day” bedreigingen) toch verwijderen.

Scanwolk

De Scanwolk is een efficiënt cluster met verschillende server-systemen gekoppeld aan het Internet, waarop de verschillende antivirussoftware van onze partners actief zijn. De Scanwolk geeft over bekende bestanden al in slechts milliseconden het antwoord en weet verdachte bestanden binnen enkele seconden te scannen en te identificeren. Daarbij kan de Scanwolk niet alleen bepalen of een bestand schadelijk is, het weet ook welke bestanden legitiem (veilig) zijn (zie ook Whitelisting, pagina 13). Ter vergelijking, de meeste traditionele antivirussoftware heeft alleen definities over bedreigingen en maakt soms ook fouten op legitieme Windows bestanden:

http://www.security.nl/artikel/31314/1/Norman_beschouwt_Windows_als_malware.html

Eén keer scannen

Terwijl Hitman Pro 3 de herkenning van 7 verschillende antivirusprogramma's heeft hoeft het dankzij de Gedragsscan en de Scanwolk de computer slechts één keer te controleren.

Centraal systeem

SurfRight is het eerste en enige bedrijf dat een Scanwolk heeft. Er zijn andere beveiligingsbedrijven die ondertussen ook aan "cloud computing anti-malware" of "cloud antivirus" doen maar zij bundelen geen meerdere beveiligingsbedrijven zoals de Scanwolk van SurfRight. De Scanwolk lijkt nog het meest op VirusTotal maar de Scanwolk is geïntegreerd in een gebruikersvriendelijke antivirusoplossing om automatisch en in luttele seconden de verdachte bestanden te identificeren.

Door 7 verschillende beveiligers te bundelen heeft Hitman Pro 3 in principe de virusherkenning van al deze onderzoekers. Waar de topman van beveiligingsreus McAfee op 22 april 2009 nog over droomt, heeft SurfRight in 2008 al gerealiseerd:

> http://techworld.nl/article/6741/mcafee-wil-wereldwijd-knmi-voor-security.html
>
> McAfee: *"Een centraal systeem in de cloud moet er in de toekomst voor gaan zorgen dat securitysoftware veel beter wordt in het anticiperen van dreigingen."*

Virusherkenning op inhoud

Veel bekende antispyware of antimalware programma's zoeken ook naar bestanden en registersleutels op basis van naam. Maak bijvoorbeeld in het Windows register onder HKEY_CLASSES_ROOT bijvoorbeeld de sleutel XML.XML aan en erg veel opschoonsoftware (zoals Malwarebytes' Anti-Malware en Ad-aware) zal het verwijderen, ook al heb je dat zelf aangemaakt. Hier is op zich niets mis mee mits fabrikanten deze definitie zorgvuldig afwegen (zoals het voorbeeld), maar het zou natuurlijk voor problemen met legitieme software kunnen zorgen. Verder zijn de meeste registersleutels gewoon ongevaarlijk als ze wees zijn (als het bijbehorende bestand – de echte bedreiging – niet meer op het systeem staat).

Hitman Pro 3 is anders en werkt vanuit de echte bedreiging. Het zoekt naar malware die een directe bedreiging is, of in de toekomst kan worden. Zo analyseert het bijvoorbeeld eerst waar een bestand waarschijnlijk vandaan is gekomen, wat voor activiteit het heeft, of ze voor de gebruiker zichtbaar en eenvoudig te verwijderen zijn en hoe deze bestanden technisch zijn opgebouwd. Het zoekt in PE bestanden naar betrouwbare certificaten, bepaalt de gegevensdichtheid, analyseert de PE headerinformatie (zoals de importtabellen) en herkent het veel in malware voorkomende technische fouten en afwijkingen. Het laat indien nodig daarna de verdere inhoud door de Scanwolk controleren. Zo vangt Hitman Pro 3 ook malware die op niet standaard locaties staan of een willekeurige naam hebben. Hitman Pro 3 zoekt dynamisch naar de bijbehorende registersleutels en snelkoppelingen en verwijdert of herstelt deze.

Directe disktoegang

Hitman Pro 3 leest vanaf versie 3.5 bestanden en registerinformatie ruw van de disk in plaats van de gangbare Windows Application Programming Interfaces (API's) te gebruiken. Geavanceerde malware filtert Windows API's en voorkomt dat antivirussoftware de infecties überhaupt kan vinden. Er gaat malware rond (zoals TDS rootkit en varianten) die zelfs nog niet door de nieuwe 2010 versies van de gerenommeerde fabrikanten wordt gezien – de producten die je in de winkel vindt zijn allemaal nog steeds afhankelijk van Windows API's. Hitman Pro 3.5 maakt hier nauwelijks gebruik van en zoekt o.a. naar verschillen tussen de ruwe data op de disk en wat de Windows API's teruggeven. Verschillen tussen ruwe data en de door Windows beheerde gegevens (API's) zijn een indicatie dat de computer geïnfecteerd is en dat de objecten onder deze verhullingtechnologie verdacht zijn – deze objecten zijn vaak niet voor computergebruikers en de meeste antivirussoftware zichtbaar en daarom per definitie verdacht.

Zonder updates toch altijd up-to-date

Omdat de verschillende antivirussoftware van onze partners niet op de computer van de eindgebruiker actief is, maar op server-systemen in de Scanwolk op het Internet, hoeft de Hitman Pro 3 software eigenlijk zelden bijgewerkt te worden. Het bijwerken van de virusdefinities gebeurd in de Scanwolk automatisch zodra ze beschikbaar zijn. Voor Prevx heeft de Scanwolk een real-time databaselink voor directe up-to-date gegevensuitwisseling.

Nieuwe bedreigingen

Het duurt overigens in het algemeen 2 tot 8 dagen voordat een nieuwe bedreiging door fabrikanten van antivirussoftware wordt ontdekt. Specialisten moeten de nieuwe bedreigingen dan onderzoeken, een herkenning- en verwijderdefinitie maken en deze naar eindgebruikers verspreiden.

Wij kunnen dit meten omdat Hitman Pro 3 dankzij de Gedragsscan ook bedreigingen vindt die de 7 gerenommeerde antivirussoftware in de Scanwolk nog niet direct kennen.

Bestanden die na ontvangst in de Scanwolk onbekend blijven worden periodiek opnieuw gescand – als de definities in de Scanwolk zijn bijgewerkt. Hierdoor worden de nieuwe bedreigingen op een later tijdstip alsnog geïdentificeerd. In de tussentijd geeft de Gedragsscan met Early Warning Scoring (zie pagina 22) de eindgebruiker handvaten om zelf een gefundeerde beslissing te nemen – het nieuwe gevaar te negeren of direct te verwijderen.

Wordt niet geïnstalleerd

De Hitman Pro 3 software voor de eindgebruiker installeert niets op het systeem van de gebruiker – de software belast de computer dus niet doorlopend. Maar om ervoor te zorgen dat gebruikers de software kunnen terugvinden kopieert Hitman Pro zichzelf wel naar de harddisk van de computer, maakt het een snelkoppeling op het bureaublad en een zogenaamde uninstall entry zodat het bestand op de reguliere wijze kan worden verwijderd (via Software in het Configuratiescherm van Windows). Maar in principe werkt Hitman Pro 3, in tegenstelling tot alle andere antimalwaresoftware, ook gewoon van een USB stick. Het is maar 1 enkel bestand.

Geen conflicten met andere antivirusprogramma's

Zoals iedereen weet kan men normaal geen 2 antivirusprogramma's naast elkaar gebruiken. In tegenstelling tot traditionele antivirusprogramma's installeert Hitman Pro 3 geen API-hooks en luistert het dus niet op Windows API's. Hierdoor conflicteert het dus niet met (real-time) antivirussoftware dat eindgebruikers al op hun computer hebben. De Gedragsscan van Hitman Pro 3 heeft deze technieken niet nodig om malware te herkennen en is dus een ideaal hulpmiddel om als extra controle (second opinion) te fungeren.

Razendsnel

Hitman Pro 3 is al binnen enkele minuten klaar waar traditionele antivirussoftware vaak tientallenminuten over doen. Om dit te bereiken hebben we een efficiëntere aanpak en technieken ontwikkeld.

Fysieke sectorvolgorde

De harde schijf in een computer raakt snel gefragmenteerd doordat er voortdurend bestanden bij komen en af gaan. De harde schijf moet daarom regelmatig gedefragmenteerd worden – defragmenteren zet de bestanden op de harde schijf in een efficiëntere volgorde waardoor het werken met de computer vlot blijft.

Hitman Pro 3 is echter niet afhankelijk van de bestandsvolgorde op de harde schijf. In tegenstelling tot traditionele antivirussoftware scant Hitman Pro 3 het systeem niet in alfabetische volgorde maar leest het eerst de ruwe gegevens in de Master File Table uit en sorteert het de aangetroffen bestanden op fysieke volgorde (sectoren). Zo hoeft de leeskop van een gangbare harde schijf in veel minder bewegingen over de disk, ongeacht de fragmentatiestatus van de harde schijf.

Whitelisting

Een groot probleem, dat gelukkig niet zo heel vaak voorkomt, is als antivirusprogramma's legitieme bestanden verwijderen. Vooral als het Windows bestanden betreft kan het dan gebeuren dat essentiële onderdelen van de PC niet meer opstarten. Om dit te voorkomen weet Hitman Pro 3 welke bestanden standaard bij het systeem horen doordat het een uitgebreide witte lijst met zogenaamde hashes van deze legitieme bestanden aan boord heeft. Hitman Pro heeft o.a. hashes van standaard installaties van Windows 2000 tot Windows 7, Office 2000 tot 2007 en alle updates en service packs aan boord, zodat Hitman Pro 3 deze bestanden na een korte controle niet door de Gedragsscan hoeft te laten analyseren.

Controle van digitale handtekeningen

Veel moderne software is digitaal ondertekend met een zogenaamd Authenticode certificaat. Een dergelijk certificaat kost geld, wordt alleen door betrouwbare instanties vertrekt en er zijn (strenge) eisen aan verbonden. Hitman Pro 3 heeft een lijst van certificaten van betrouwbare fabrikanten aan boord – zoals Microsoft, Adobe, etc. Als een dergelijk certificaat wordt aangetroffen wordt het bestand niet verder door de Gedragsscan geanalyseerd.

Direct gevaar

Hitman Pro 3 detecteert alleen malware dat direct of in de toekomst een bedreiging vormt. Dit betekent dat de malware actief moet zijn, automatisch start of een snelkoppeling heeft. Hitman Pro 3 gaat niet zoals andere antivirussoftware zomaar alle bestanden op een disk controleren, want dit is praktisch gezien ook niet nodig. Hitman Pro 3 is een redmiddel om computers snel en direct te bevrijden van bestaande en nieuwe (vaak nog onbekende) malware.

Gebruikersvriendelijk

Het bedienoppervlak van Hitman Pro 3 is bijzonder gebruikersvriendelijk. Geen overdaad aan instellingen, knoppen, geen onoverzichtelijke schermen of moeilijke termen. Het is daarom ook geschikt voor mensen die geen affiniteit met computerbeveiliging hebben, dus ook beginnende gebruikers en je grootouders kunnen er eenvoudig mee overweg.

Richtlijnen voor het testen van Hitman Pro

Lees dit hoofdstuk geheel door als u een goede on-demand test met Hitman Pro wilt uitvoeren.

Traditioneel wordt de detectiegraad van antivirussoftware getest door een grote hoeveelheid geverifieerde virusbestanden (samples) te scannen en daarna het detectiepercentage te noteren. Bij een zogenaamde on-demand test worden de samples in een map op een reguliere Windows XP testcomputer gekopieerd waarna de antivirussoftware wordt gevraagd de inhoud te scannen.

Echter, de manier waarop de Gedragsscan werkt zorgt ervoor dat Hitman Pro niet alle samples van een on-demand test als schadelijk zal opmerken. Dit komt omdat er op de testcomputer geen actieve infectiesporen aanwezig zijn die wel op een realistisch besmette computer bestaan. De Gedragsscan bestaat grotendeels uit associatiewinning waardoor schadelijke bestanden die geen directe bedreiging vormen (bijvoorbeeld niet geladen of actief zijn of niet automatisch opstarten) niet direct als kwaadaardig worden bestempeld.

Hitman Pro scant alleen naar actieve en (via snelkoppeling handmatig of) automatisch startende Portable Executable bestanden (zoals EXE, DLL, SYS). Hitman Pro zal geen schadelijke bestanden ontdekken die niet of nooit (automatisch) actief worden, niet toegankelijk zijn via een snelkoppeling en niet op gangbare (systeem) locaties staan. Dit betekent ook dat Hitman Pro o.a. geen documenten scant en deze ook niet door de Scanwolk laat inspecteren op schadelijk macro's of scripts.

Eigenlijk betekent dit dat producttesters een testcomputer echt moeten infecteren (telkens een virussample activeren) om de werking van Hitman Pro te testen. Bij een dergelijke vergelijkende test zal ook duidelijk worden dat de meeste concurrerende antivirussoftware, in tegenstelling tot Hitman Pro, sommige actieve bedreigingen niet kan verwijderen of ze zelfs niet kan ontdekken. Ook zal dan duidelijk worden of antivirussoftware gewijzigde Windows systeembestanden, registersleutels, snelkoppelingen en systeeminstellingen kan herstellen – functionaliteit die gangbare antivirussoftware ontbeert maar waarmee Hitman Pro juist mee is uitgerust. Probeer maar eens een actieve TDSS rootkit met een traditioneel antivirusprogramma te verwijderen.

Actieve internetverbinding

Om tijdens het testen gebruik te maken van de Scanwolk (cloud computing) moet het testsysteem een actieve internetverbinding hebben. Hitman Pro zal standaard via poort 443 (HTTPS) met de Scanwolk communiceren (of poort 80 (HTTP) indien SSL is uitgeschakeld bij de Instellingen).

Toch een on-demand scan uitvoeren

Recentelijk is Hitman Pro 3.5 uitgerust met een speciale functie om alle (PE) bestanden in een map te scannen. Door in de configuratie van Hitman Pro (zie de knop Instellingen) de functie **Toon 'Scan met Hitman Pro' optie bij bestanden en mappen in Windows Verkenner** in te schakelen kan de producttester toch een map met infectiebestanden scannen – dus een klassieke on-demand scan uitvoeren. Let op dat de map op de lokale computer moet staan en dat eventuele submappen niet worden meegenomen tijdens deze scan.

Om een map met bestanden te scannen klikt de producttester met de rechter muisknop op de lokale map en kiest dan uit het menu de optie **Scan met Hitman Pro**.

Definitieloos

Omdat de ingebouwde scanner van Hitman Pro (in tegenstelling tot traditionele antivirussoftware) geheel niet met virusdefinities werkt zal bij afwezigheid van een internetverbinding alleen bestanden met veel in malware voorkomende afwijkingen worden weergegeven. Rootkit-infectiebestanden zullen bijvoorbeeld als "Verdacht" worden gemarkeerd. Bij afwezigheid van een internetverbinding kunnen producttesters ook het Early Warning Scoring (EWS) bij Instellingen inschakelen, waarna Hitman Pro meer potentieel schadelijke software kan weergeven.

Vanwege het afwijkende ontwerp van de scanner in Hitman Pro kan het, bij afwezigheid van een internetverbinding, niet met traditionele antivirussofware vergeleken worden.

Omdat Hitman Pro definitieloos is kan het echter geen registersleutels, snelkoppelingen of andere weesbestanden verwijderen als de bijbehorende infectiebestanden niet meer op de computer aanwezig zijn. Hitman Pro zoekt intelligent naar o.a. registersleutels en snelkoppelingen die naar schadelijke bestanden wijzen. Zonder de schadelijke bestanden zal Hitman Pro geen losse registersleutels en snelkoppelingen verwijderen – het heeft geen geldige reden om deze te verwijderen. Hitman Pro zal niet alleen infectiebestanden en registersleutels verwijderen maar kan, als ze bij Windows horen, ook van originele installatieschijf herstellen of repareren.

Second opinion met een traditioneel antivirusprogramma

Als producttesters een traditioneel (op virusdefinities gebaseerd) antivirusprogramma willen gebruiken om naar achtergebleven sporen te zoeken, wees er dan zeker van dat de log-bestanden van deze programma's goed geïnterpreteerd worden. Pas als Hitman Pro helemaal klaar is (en de computer is ook, indien gevraagd, opnieuw opgestart) en het geen infectiebestanden meer vindt, zullen er geen malware-bestanden in het geheugen actief mogen zijn. Kijk dus goed wat de andere virusscanners hierna nog naar boven halen. Registersleutels en snelkoppelingen zonder de (PE) infectiebestanden, als ook cookies, zijn geen echte bedreigingen en mogen dus ook niet als zodanig in een test als infectie worden meegenomen.

We adviseren producttesters om dergelijke tests ook in "omgekeerde" volgorde te doen. Maak een geïnfecteerd computersysteem eerst met een ander antivirusprogramma schoon en voer daarna nog de second opinion uit met Hitman Pro. Dit is namelijk hoe Hitman Pro normaal gebruikt wordt. Het resultaat kan heel verrassend zijn.

Wat is nieuw in versie 3.5

Hitman Pro versie 3.0 is de eerste Hitman Pro gemaakt door SurfRight B.V. Technisch gezien is het ook de eerste (en nog steeds enige) anti-malware met een Gedragsscan en een Scanwolk, waar meerdere beveiligers dankzij cloud computing, zorgen voor up-to-the-minute virusdetectie en identificatie. Hierdoor is Hitman Pro 3 zonder twijfel nog steeds ongeëvenaard in het snel vinden en verwijderen van actuele bedreigingen.

Met versie 3.5 leggen we de lat nog hoger. Het hele programma is volledig opnieuw gebouwd. Dit hebben we gedaan om eigenlijk maar 1 reden: andere antivirussoftware maakten doorlopend zogenaamde false positives op de Hitman Pro 3 software. Hierdoor werd het regelmatig onterecht als virus gemarkeerd. Keer op keer werden de fouten door de andere beveiligers natuurlijk wel hersteld, maar dergelijke ongelukkige situaties scheppen geen vertrouwen bij eindgebruikers. Om dit probleem op te lossen hebben we besloten niet langer het door beveiligers ogenschijnlijk gevreesde programmeertaal AutoIt Script in (delen van) Hitman Pro te gebruiken.

In een zeer korte tijd heeft een nieuw ontwikkelteam daarom een volledig nieuw programma in het vertrouwde C++ gebouwd: Hitman Pro versie 3.5. En natuurlijk heeft het nieuwe team tijdens de ontwikkeling ervan naar mogelijk technische, functionele en esthetische verbeteringen gekeken.

Gedragsscan

De unieke Gedragsscan is de basis van Hitman Pro 3. Het weet razendsnel schadelijke en legitieme software te onderscheiden, zonder hierbij gebruik te maken van traditionele virusdefinities.

Directe disktoegang

Hitman Pro 3.5 leest bestanden en registerinformatie nu rechtstreeks van de harde schijf. Normaal gesproken worden hier gangbare Windows Application Programming Interfaces (API's) voor gebruikt.

Geavanceerde malware filtert Windows API's en voorkomt dat antivirussoftware de infecties überhaupt kan vinden. Er gaat malware rond (zoals TDS rootkit en varianten) die zelfs nog niet door de aankomende (jaar 2010) versies van de gerenommeerde fabrikanten wordt gezien. De aankomende producten die je in de winkel vindt zijn allemaal afhankelijk van Windows API's. Hitman Pro 3.5 maakt hier nauwelijks gebruik van en zoekt o.a. naar verschillen tussen de ruwe data op de schijf en wat de Windows API's teruggeven.

Omdat Hitman Pro 3.5 nu – buiten gangbare Windows API's om – direct van de harde schijf leest, wordt het ook niet meer door traditionele antivirussoftware op de computer gehinderd (vertraagd).

Multithreading

De Gedragsscan is nu volledig multithreaded. Dit betekent dat Hitman Pro 3.5 de vele classificatietaken efficiënt over de beschikbare systeembronnen verdeeld. Zo verloopt o.a. het raadplegen en uploaden van bestanden naar de Scanwolk nu ook gelijktijdig met andere classificatietaken. De voortgang van deze activiteiten worden live in het scanoverzicht weergegeven. Verdachte bestanden zullen dankzij multithreading nu ook veel eerder worden getoond.

Hitman Pro 3.5 is op snelle computersystemen nu binnen 1 minuut klaar. De gebruiker weet dan precies of het systeem besmet is. Nog nooit eerder was antivirussoftware zo snel.

Bestandscompressie

Versie 3.0 voorkwam dat er onnodig grote bestanden naar de Scanwolk werden gestuurd om bandbreedte te besparen. In Hitman Pro 3.5 is deze beperking opgeheven want verdachte bestanden groter dan 128 KB worden nu eerst gecomprimeerd alvorens ze naar de Scanwolk te sturen. Hierdoor worden rogue antivirusprogramma's van ruim 20 MB nu ook snel geïdentificeerd.

Beveiligde verbinding (SSL)

Onbekende verdachte bestanden worden via een veilige versleutelde verbinding (SSL) naar de Scanwolk verstuurd. Hierdoor kan de communicatiestroom niet meer door eventuele hackers worden bekeken. Deze functie staat natuurlijk standaard ingeschakeld.

Verbeterde PE heuristiek

De Gedragsscan is o.a. gespecialiseerd in het analyseren van uitvoerbare computerbestanden, zogenaamde Portable Executables (PE). Dit zijn doorgaans EXE, DLL en SYS bestanden. In Hitman Pro 3.5 wordt van deze bestanden niet alleen de gegevensdichtheid (entropy) bepaald (een indicatie dat een bestand expres tegen virusonderzoek is versleuteld) maar worden ook de import-tabellen geanalyseerd en veel in malware voorkomende afwijkingen ontdekt. In versie 3.5 analyseert het nu ook de afzonderlijke data directories en kent het debug-informatie.

Gossip Rating

Elke week verspreiden cybercriminelen nieuwe nep-antivirussoftware. Deze zogenaamde "rogues" worden door de criminelen gemaakt om computergebruikers te overtuigen dat de computer geïnfecteerd is. Om het vertrouwen van de gebruiker te winnen zien ze er vaak erg professioneel uit. Om deze nep-infecties te verwijderen wordt van de gebruiker natuurlijk betaling verwacht, het liefst met credit card.

Antivirussoftware van de vele virusbestrijders doen hun uiterste best om dergelijke frauduleuze nep-software te herkennen. Maar omdat er zo vaak nieuwe varianten verschijnen duurt het dagen voordat de professionals ze opmerken en een oplossing hebben gemaakt. In de tussentijd debatteren verschillende websites en forums over computerbeveiliging echter al direct over de nieuwste nep-antivirus en nep-antispyware.

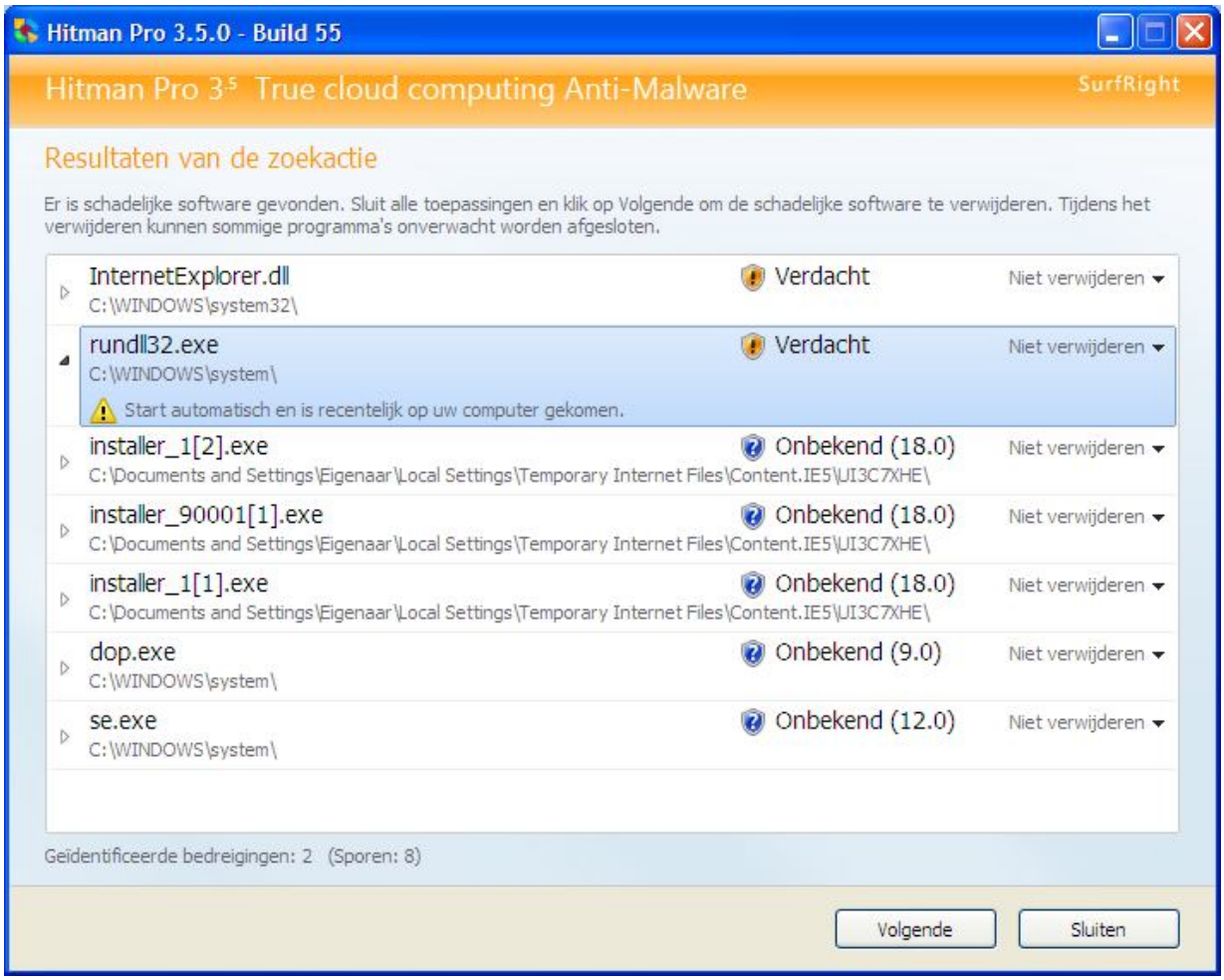
In versie 3.0 van Hitman Pro introduceerden we naast de Gedragsscan ook het Security Gossip systeem. Hiermee raadpleegde Hitman Pro naast de Scanwolk ook verschillende zoekmachines op internet, om te kijken of er over de aangetroffen software op beveiligingswebsites en forums wordt gedebatteerd. Hitman Pro 3.0 deed dat autonoom maar vanaf versie 3.5 wordt dit centraal gedaan, waar we de techniek hebben verfijnd en een stuk efficiënter hebben gemaakt. Deze nieuwe centrale functie hebben we Gossip Rating genoemd en de ontvangen waarderingen worden o.a. ook aan het nieuwe Early Warning Scoring systeem teruggekoppeld, zodat Hitman Pro 3.5 de nieuwste nep-scanners kan verwijderen.

Met de Gossip Rating neemt Hitman Pro 3.5 automatisch de discussies van de duizenden mensen achter beveiligingswebsites en forums mee in de bestrijding van malware op uw computer.

Early Warning Scoring

Het Early Warning Scoring systeem vervangt de Virusanalist-functie in Hitman Pro 3. Met Early Warning Scoring (EWS) wordt automatisch (nog) onbekende maar verdachte software getoond dat direct een bedreiging kan zijn. Het doel van EWS is om ervaren computergebruikers een bruikbaar middel te geven om actuele (maar bij virusbestrijders nog onbekende) bedreigingen direct te kunnen verwijderen.

EWS is mogelijk dankzij de innovatietechnologie achter de Gedragsscan. Om EWS te gebruiken moet de functie handmatig worden ingeschakeld (bij Instellingen). Hierdoor kunnen de allernieuwste bedreigingen worden gedetecteerd die de vele virusscanners in de Scanwolk nog niet kennen. EWS toont naast de gevarenscore ook de reden waarom een bestand potentieel gevaarlijk is.

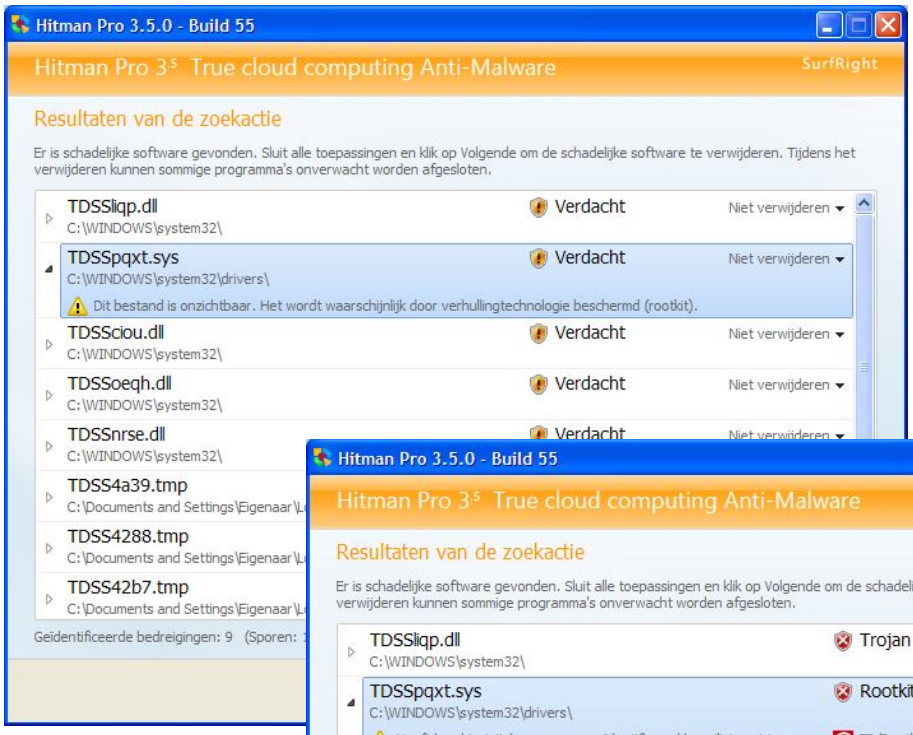


Early Warning Scoring kan via de knop Instellingen op het welkomstscherm worden ingeschakeld.

Scannen zonder internetverbinding / malware verwijderen zonder licentie

Early Warning Scoring (EWS) zorgt ervoor dat Hitman Pro 3.5 ook schadelijke software kan vinden als er geen internetverbinding beschikbaar is (de internetverbinding kan bijvoorbeeld door malware zijn uitgeschakeld).

Hitman Pro 3.5 kan malware verwijderen op computers zonder internettoegang. Hiervoor moet Early Warning Scoring (EWS) ingeschakeld zijn.



Early Warning Scoring **zonder** internetverbinding

Voorbeeld: TDSS rootkit

Early Warning Scoring **met** internetverbinding

Repareren onveilige DNS-instellingen

In versie 3.5 hebben we een universele controle voor de DNS-instellingen toegevoegd. Een onveilige DNS-server kan ervoor zorgen dat websites over computerbeveiliging niet meer bereikbaar zijn. Ook kan het de gebruiker tijdens het online bankieren ongemerkt naar een namaakpagina van zijn bank doorsluizen. Om een onveilig DNS-serveradres te ontdekken raadpleegt Hitman Pro publieke zwarte lijsten.

Als één van de netwerkverbindingen een DNS-serveradres gebruikt dat op de zwarte lijst staat dan zal Hitman Pro voorstellen de onveilige gegevens te herstellen naar veilige adressen: DHCP indien de computer automatisch een IP-adres ontvangt, of bij een statisch adres de DNS-servergegevens van het vertrouwde OpenDNS.

Repareren onveilige proxy-instellingen

Diverse Trojaanse paarden installeren lokale proxyservers en bij het verwijderen van deze schadelijke software blijft de proxyserver-instelling achter, met als gevolg dat Internet Explorer en andere programma's niet meer met internet kunnen communiceren. Hitman Pro 3.5 merkt automatisch als de computer een lokale proxyserver gebruikt die niet meer aanwezig is en zal de verbinding met het internet herstellen.

Repareren ongeldige Winsock LSP chain

Hitman Pro 3.5 is ook in staat om fouten met betrekking tot de zogenaamde "Winsock LSP chain" te repareren. Met Winsock kunnen programmeurs geavanceerde internettoepassingen maken om daarmee gegevens te verzenden die onafhankelijk zijn van het gebruikte netwerkprotocol. Het komt voor dat Trojaanse paarden (of andere malware) deze Windows-functionaliteit misbruiken om gegevens over u of van uw computer te stelen. Als er infectiebestanden in de "Winsock LSP chain" waren opgenomen dan wordt deze opnieuw ingesteld om te voorkomen dat de internetverbinding na het verwijderen van de infectie niet meer functioneert.

Crusader

De Crusader is de interne naam van het onderdeel dat verantwoordelijk is voor het verwijderen van schadelijke software. In opdracht van Hitman Pro verwijdert het schadelijke bestanden, registersleutels en snelkoppelingen. In versie 3.5 is de verwijdermodule uitgebreid met een aantal nieuwe innovatieve technieken.

Fysieke uitschakeling

Alle schadelijk software wordt nu ook direct (op sectorniveau) op de harde schijf uitgeschakeld, zodat deze bestanden onmogelijk opnieuw actief kunnen worden.

Boot-time Service

De Bootdeleter is een belangrijk onderdeel van de Crusader. Het verwijderd tijdens het opstarten van de computer de eerder door Hitman Pro uitgeschakelde en achtergebleven infectiebestanden. Versie 3.5 heeft een extra service gekregen die – in aanvulling op de "native NT" Bootdeleter – ook malware gerelateerde registersleutels en snelkoppelingen verwijderd. Hierdoor wordt resistente schadelijke software - na het opnieuw starten van de computer – direct volledig verwijderd.

Herstellen van kritieke systeembestanden (WPF)

Om de stabiliteit van Windows te waarborgen worden geïnfecteerde maar kritieke systeembestanden natuurlijk niet zomaar verwijderd. Hitman Pro 3.5 gaat op zoek naar een veilig exemplaar en vervangt hiermee de geïnfecteerde versie.

Als er geen veilig exemplaar op de lokale harde schijf wordt gevonden dan krijgt de gebruiker de mogelijkheid om een veilig origineel systeembestand van de Windows installatie cd-rom te gebruiken.

In het geval het kritieke systeembestand niet kan worden hersteld blijft het systeem werkend, al blijft het geïnfecteerd. Deze methode voorkomt "de operatie is geslaagd, maar helaas is de patiënt overleden".

Bijgewerkte ingebouwde whitelist

In Hitman Pro 3.5 is de ingebouwde witte lijst uitgebreid met vele talen zodat we ook buitenlandse systemen razendsnel kunnen controleren. En de witte lijst bevat nu ook gegevens over de 64-bit (x64) versies van Windows XP, Vista en 2008 als ook gegevens over Windows 7. Niet alleen versnelt de witte lijst het scanproces aanzienlijk, maar hierdoor is het ook onmogelijk dat er ooit veilige Windows-bestanden door Hitman Pro worden verwijderd.

Bedienoppervlak

Hitman Pro 3.5 heeft een nieuwe GUI gekregen (Graphical User Interface). Omdat het nieuwe ontwikkelteam niet aan de beperkingen van AutoIt Script was gebonden is er gekeken om een inzichtelijker en eenvoudiger bedienoppervlak te creëren. Het nieuwe bedienoppervlak maakt de gegevens inzichtelijker, eenvoudiger en voelt sneller.

Meer controle

In Hitman Pro 3 kon de gebruiker niet makkelijk zelf kiezen welke (door professionele virusbestrijders als schadelijk geïdentificeerde) bestanden op de computer mochten blijven en was het onduidelijk welke verdachte bestanden naar de Scanwolk werden gestuurd.

In Hitman Pro 3.5 kan – zonder in te boeten aan de bijzonder eenvoudige bediening – elke gebruiker nu zelf aangeven welke schadelijke software wordt verwijderd en welke onveilige instellingen worden hersteld. Ook is het inzichtelijker welke verdachte bestanden naar de Scanwolk gaan en kan het verzenden individueel worden afgebroken.

Zichtbaarheid beveiligingspartners

In het scanoverzicht worden nu de afzonderlijke virusnamen van de verschillende partners getoond. Zo is inzichtelijk welke virusbestrijder in de Scanwolk een bestand als schadelijk heeft geïdentificeerd.

Nieuw product-logo

Met de komst van Hitman Pro 3.5 introduceren we ook een nieuw Hitman Pro logo / pictogram:

Hierin symboliseert de “pac man” in het midden de statistische wijze waarop de Gedragsscan werkt maar ook het opeten van malware. De “taartpunt” symboliseert daarbij ook het breed “scannen”. De omringende gekleurde elementen – waaronder de hoeksteen – symboliseren de meerdere verschillende beveiligingspartners en de complete herkenning in de Scanwolk. De verschillende kleuren worden ook gebruikt in het Microsoft Windows logo, het besturingssysteem waar Hitman Pro voor bedoeld is.

Het nieuwe Hitman Pro logo past bij de nieuwe uitstraling die we het programma hebben gegeven.

Revisiegegevens Productbeschrijving

Versie	Auteur	Opmerkingen
1.0	ML	Initiële uitgave.
1.1 – 20090710	ML, HW	Diverse tekstuele wijzigingen.
1.2 – 20091012	ML, HW	Diverse aanvullingen en tekstuele wijzigingen.