SurfRight

Command-Line Reference for Network Managers

Table of Contents

Introduction to HitmanPro

HitmanPro 3 is a solution to counter malicious software such as viruses, spyware, Trojans, worms, adware, bots and rootkits, also known as malware (malicious software). HitmanPro 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. HitmanPro 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 HitmanPro 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]

Cyveilance "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 HitmanPro 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
[2] http://www.cyveillance.com/web/docs/WP_CyberIntel_H1_2009.pdf
[3] http://www.damballa.com/downloads/press/Failsafe_3_(PR_FINAL_2009-3-2).pdf
[4] http://blog.fireeye.com/research/2008/11/does-antivirus-stop-bots.html
[5] http://www.virusbtn.com/conference/vb2009/abstracts/Mandl.xml
[6] http://www.virusbtn.com/vb100/index

Behavioral Scan

HitmanPro 3 is an on-demand signature-less behavioral and cloud based malware scanner. This scan is the result after meticulously analyzing the behavior of over 300,000 malware samples. Using details from this research, HitmanPro essentially generates a threat severity score for each file it encounters. This score is based on analysis of each scanned file's structure while determining its origin, visibility, activity, reputation, boot survivability and relation to other file and registry objects and their reputations. Reputations are provided by our Scan Cloud infrastructure where also third party expertise reside. 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. HitmanPro 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 HitmanPro's malware removal engine Crusader (which we specifically designed to cope with the most resilient threats).

Fast Scanning

HitmanPro 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 HitmanPro 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). HitmanPro 3 will perform disk, registry, network (for example cloud scanning) and internal analysis tasks simultaneously.
- HitmanPro 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.

Cloud Assisted Miniport Hook Bypass

The toughest types of malware are rootkits. Rootkits embed themselves deep in the operating system where they hide for 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 the TDSS family (TDL, Alureon.DX, Olmarik) and variants of Mebroot and Sinowal work on both 32-bit and 64-bit versions of Windows and infect the Master Boot Record (MBR). This means that these so called Bootkits start before Windows boots up, which gives the bootkit an obvious advantage. Any protection mechanism imposed by Windows (or antivirus that is loaded by Windows) can be defeated (the program that is started first, can have control over the others).

Once Windows is booting, the rootkit attaches a filtering mechanism to the hard disk driver. This filter gives the rootkit complete control over the hard drive. For example, when an antivirus tries to read the MBR (sector 0) of the hard drive (to see if it is infected), the rootkit will simply serve a regular MBR so that it appears that the MBR is clean. Hence, the rootkit is undetected.

Now in order to read the actual infected MBR you need get around the rootkit's filtering mechanism. For this you need to know two things:

1. The hard disk miniport driver that is hooked (e.g. atapi.sys, iaStor.sys, nvstor32.sys, amdsata.sys, etc.)
2. How the rootkit is hooking into it.

When you know the exact hard disk driver that is in use, you are able to communicate directly with it, reading around the hooks of the rootkit.

The problem is that there are literally thousands of different brands, types and versions of hard disk drivers and they all need to be addressed differently. This is where Cloud Assisted Miniport Hook Bypass comes in.

Our proprietary **Cloud Assisted Miniport Hook Bypass (CAMHB)** 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 filtering and effectively reading the actual infected sectors. This works for ANY hard disk driver and not just the common ones.

Cloud Assisted Miniport Hook Bypass collectively helps HitmanPro users to combat the toughest malware threat: Rootkits. CAMHB is available in HitmanPro 3.5.9 (or newer).

Scan Cloud

Cloud computing is the use of computer technology using the Internet (the term cloud is a metaphor for the Internet). Cloud-based HitmanPro 3 handles in-depth scanning of files on a remote server, rather than on a user's machine. The Scan Cloud of HitmanPro 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 HitmanPro 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 HitmanPro 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 HitmanPro 3, the Scan Cloud can be used to identify new threats on a global scale. The Behavioral Scan in HitmanPro 3 has turned every system into an in-depth malware analyzer.

Crusader

HitmanPro's Behavioral Scan also correlates objects to produce a unique malware removal and repair recipe on the fly, because nowadays, malware generates random files and registry objects on each machine it successfully infects.

The malware removal engine in HitmanPro is called Crusader and will thoroughly kill malicious files in memory and deploys countermeasures when it detects re-infection activity. Also, threat objects on the disk are physically disabled, practically preventing them from running again on the computer. Remaining objects are cleaned during boot by Crusader's native NT bootdeleter which runs before other programs start and the desktop appears.

Unlike most other antivirus solutions, HitmanPro's Crusader is able to restore an infected Master Boot Record (MBR) and critical Windows operating system files, which make up for most of the infections nowadays – cybercriminals know it is hard for security programs to detect these and that the renowned internet security suites do not have the technology to handle and repair these infections.

Windows 7 Compatible Logo

HitmanPro is authorized by Microsoft to bear the Windows 7 Compatible Logo[7].

[7] http://www.microsoft.com/Windows/compatibility/windows-7/en-us/Details.aspx?type=Software&p=Hitman%20Pro&v=SurfRight&uid=3&l=en&pf=0&pi=2&s=Hitman&os=64-bit

HitmanPro In Your Network

Every day hundreds of thousands of home computers are infected by malware. Even though business computers and their users are often limited by policies and the network is shielded by multiple antivirus engines, intrusion detection firewalls, proxies and spam filters, virus outbreaks happen in medium or large networks too.

Version 3.5.5 and higher contains extra functionality for IT Network Managers to quickly scan (in less than a few minutes) their networks for threats. The HitmanPro 3 client software is equipped with extra command-line functions so the program can run silently and report back to a central location. This is particularly useful when administrators are faced with a virus outbreak in their organization and would like to pinpoint the computers that are infected.

Windows Server 2003

If you have a Windows Server 2003 based network, one solution to initiate a network scan is to use a Group Policy Object (GPO).

Follow this example to scan every computer on the network using a Group Policy Object (GPO):

1. Setup the share: create a network share on the server that must receive the log files. Make certain you give the **Everyone** group **Change** and **Read** permissions on this share.
2. On the Windows Server, copy the program **C:\Windows\System32\schtasks.exe** to the share. This to ensure that every computer runs the same schtasks.exe program, because the /SC switch is OS language dependant.
3. Download the 32-bit and 64-bit versions HitmanPro and follow these steps:
    a. Copy the **HitmanPro.exe** and **HitmanPro_x64.exe** programs to the share.
    b. Create a **RunHMP.bat** file in the share. The following is an example of its contents:

```
\\ServerName\ShareName\schtasks.exe /DELETE /TN "HitmanPro Scan" /F
goto %PROCESSOR_ARCHITECTURE%
:x86
\\ServerName\ShareName\schtasks.exe /CREATE /RU domain\administrator
/RP password /SC ONIDLE /I 10 /TN "HitmanPro Scan" /TR
"\\ServerName\ShareName\HitmanPro.exe /scanonly /quick
/log=\\ServerName\ShareName\%computername%.xml"
goto end
:AMD64
\\ServerName\ShareName\schtasks.exe /CREATE /RU domain\administrator
/RP password /SC ONIDLE /I 10 /TN "HitmanPro Scan" /TR
"\\ServerName\ShareName\HitmanPro_x64.exe /scanonly /quick
/log=\\ServerName\ShareName\%computername%.xml"
:end
```

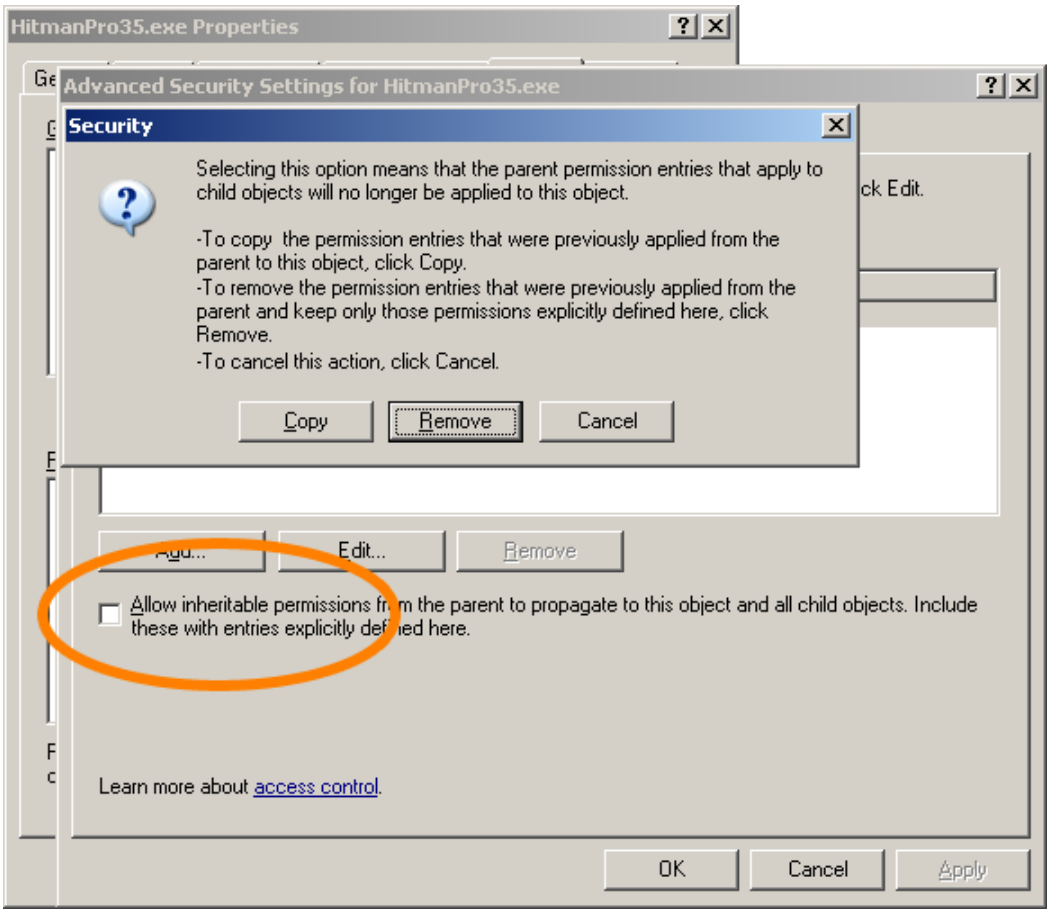
Notes: Change the script, like the **blue** data, according to your wishes and environment. To change the schedule, alter the **orange** data to your preference, for example:

- `/SC DAILY /ST 13:00:00` Scan every day at 1:00 PM
- `/SC ONCE /ST 10:00:00` Scan once at 10:00 PM
- `/SC ONIDLE /I 30` Scan when the computer is idle for 30 minutes

c. To prevent users from tampering with the necessary files, remove the default permissions on each of these files in the share:

- HitmanPro.exe
- HitmanPro_x64.exe
- RunHMP.bat
- schtasks.exe

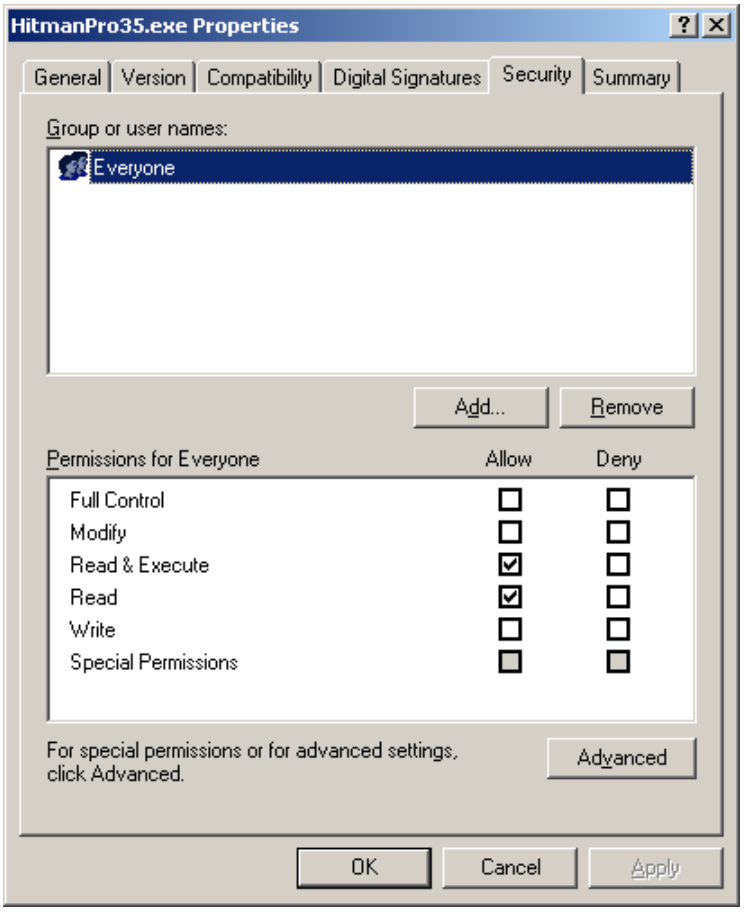
Uncheck **Allow inheritable permissions from the parent...** on the **Permissions** tab through Security > Advanced and click **Remove** on the Security dialog:



d. Click **OK**.

e. Give the **Everyone** group **Read** and **Read & Execute** permissions on each of these files:

- HitmanPro.exe
- HitmanPro_x64.exe
- RunHMP.bat
- schtasks.exe



f. Click **OK**.

4. Setup the startup script. To do this, follow these steps:

a. In the **Active Directory Users and Computers** MMC snap-in, right-click the domain name, and then click **Properties**.

b. On the **Group Policy** tab click **Open** to access the Group Policy Management snap-in.

c. Right-click the domain name and click **Create and Link a GPO Here**, and type **HitmanPro Scan** for the name of the policy.

d. Right-click the new **HitmanPro Scan** policy, and then click **Edit**.

e. Expand **Windows Settings** for **Computer Configuration**, and then click **Scripts (Startup/Shutdown)**.

f. Double-click **Startup**, and then click **Add**. The **Add a Script** dialog box is displayed.

g. In the Script Name box, type **\\ServerName\ShareName\RunHMP.bat**

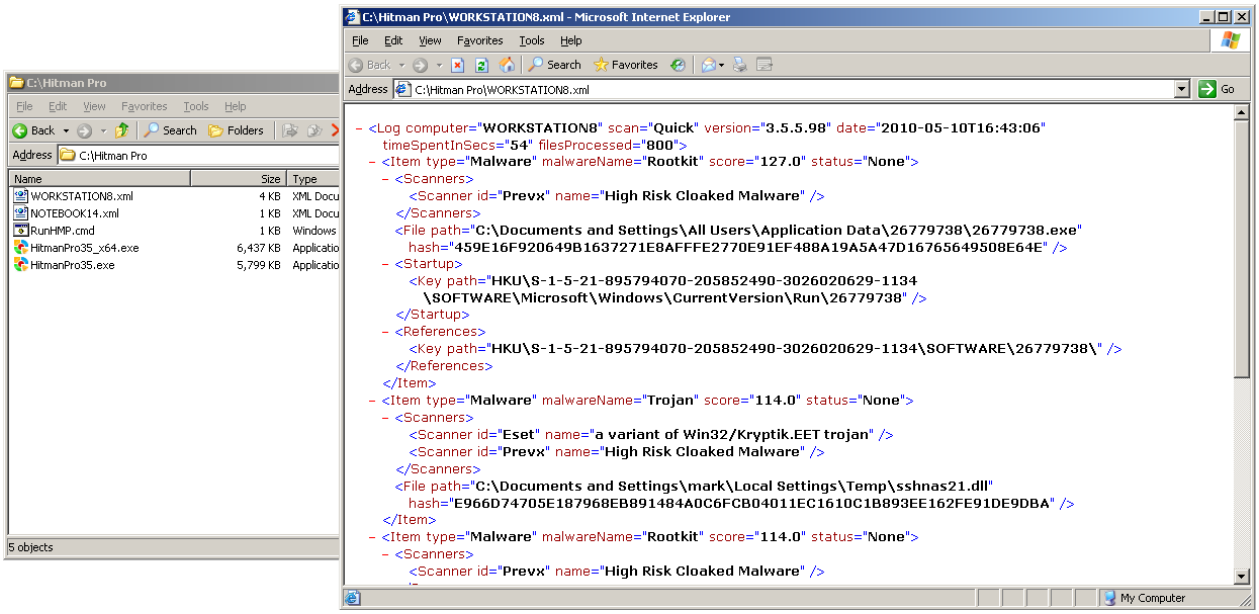
   Note: Change the **blue** data according to your environment.

h. Click **OK**, and then click **Apply**.

After you make changes to group policies, you may want the changes to be applied immediately, without waiting for the default update interval (90 minutes on domain members). So, on a regular computer (domain member), run **gpupdate.exe** to force a refresh of the Group Policy settings.

Monitor the Log Files

Monitor the \\ServerName\ShareName and watch for xml files bigger than 1 KB. These xml files contain information about infected objects – in other words, these computers are infected:



Remove the Infections

To remove the infections, visit this computer and run HitmanPro interactively as an administrator.

Windows Server 2008 R2

If you have a Windows Server 2008 R2 based network follow this example to scan every computer on the network using a Scheduled Task item in a Group Policy object (GPO):

1. Setup the share: create a network share on the file server that must receive the log files. Make certain you give the **Everyone** group **Change** and **Read** permissions on this share.

2. Download the 32-bit and 64-bit versions HitmanPro and follow these steps:

    a. Copy the **HitmanPro.exe** and **HitmanPro_x64.exe** programs to the share.

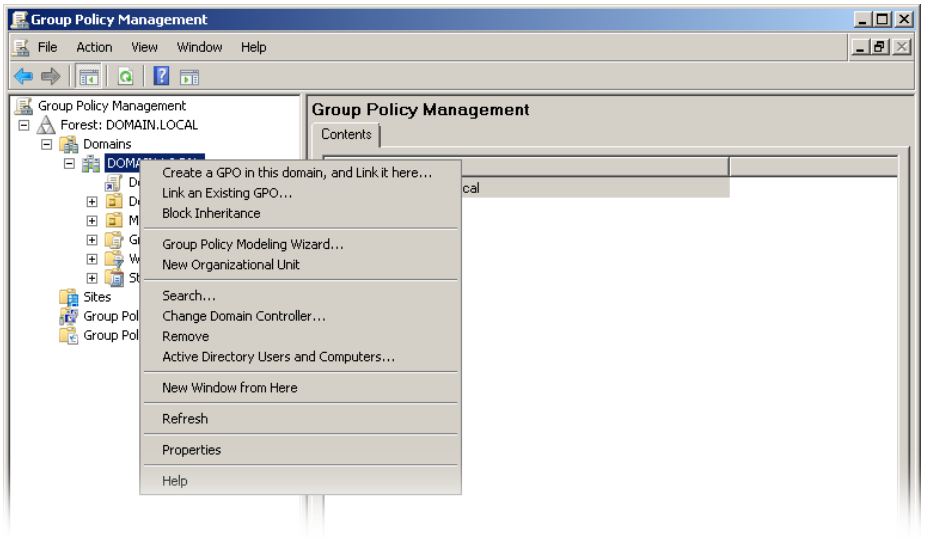
    b. Create a **RunHMP.bat** file in the share. The following is an example of its contents:

```
goto %PROCESSOR_ARCHITECTURE%
:x86
\\ServerName\ShareName\HitmanPro.exe /scanonly /quick
   /log="\\ServerName\ShareName\%COMPUTERNAME%.xml"
goto end
:AMD64
\\ServerName\ShareName\HitmanPro_x64.exe /scanonly /quick
   /log="\\ServerName\ShareName\%COMPUTERNAME%.xml"
:end
```

    Notes: Change the server name, share name and HitmanPro switches in the script according to your environment and requirements.

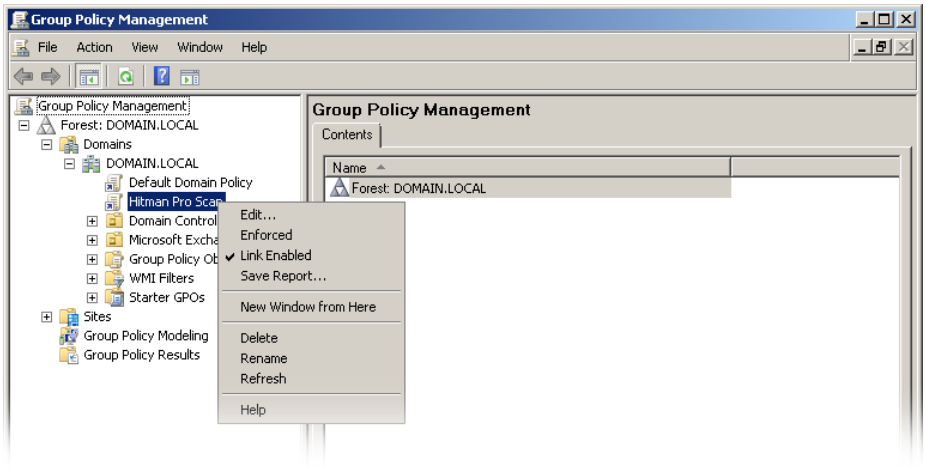
3. Open the **Group Policy Management Console** (from Start > Administrative Tools).

4. Right-click the domain name and click **Create a GPO in this domain, and Link it here**.



5. Type **HitmanPro Scan** for the name of the policy.

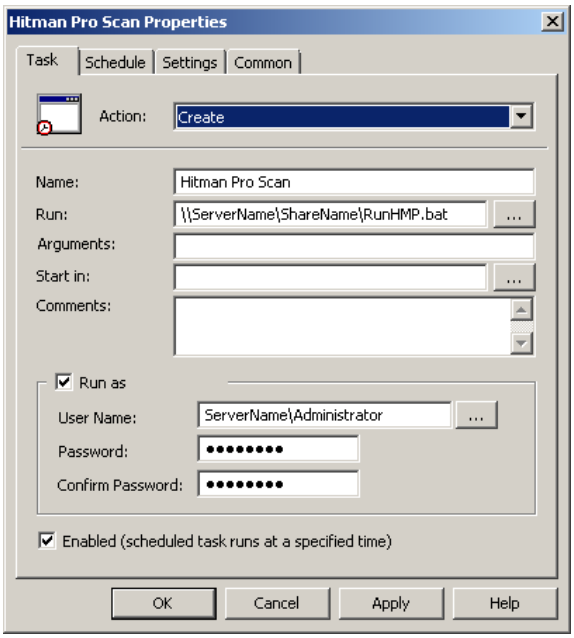
6. Right-click the new **HitmanPro Scan** policy, and then click **Edit**.



7. In the console tree under **Computer Configuration**, expand the **Preferences** folder, and then expand the **Control Panel Settings** folder.

8. Right-click the **Scheduled Tasks** node, point to **New**, and select **Scheduled Task**.

9. In the **New Scheduled Task Properties** dialog box, select the **Create** action.



10. Make certain the task will run as an administrator.

11. Configure the frequency with which to execute the task on the **Schedule** tab and click **OK**.

After you make changes to group policies, you may want the changes to be applied immediately, without waiting for the default update interval. So, on a regular computer (domain member), run **gpupdate.exe** to force a refresh of the Group Policy settings.

Monitor the Log Files

Monitor the **\\ServerName\ShareName** and watch for xml files bigger than 1 KB. These xml files contain information about infected objects – in other words, these computers are infected:

Remove the Infections

To remove the infections, visit this computer and run HitmanPro interactively as an administrator.

Integrate HitmanPro with LabTech

Whether you are a one-man break/fix shop or an established managed service provider (MSP), IT businesses benefit from the array of automation features the LabTech remote monitoring and management (RMM) platform has to offer. More info here: http://www.labtechsoftware.com/labtech-ignite.php

The following example script for use with the LabTech software will automatically download the latest version of HitmanPro (32-bit or 64-bit) on the remote computer. When done, it will scan the computer and automatically create a ticket when malware was found.

To install the script, follow these steps:

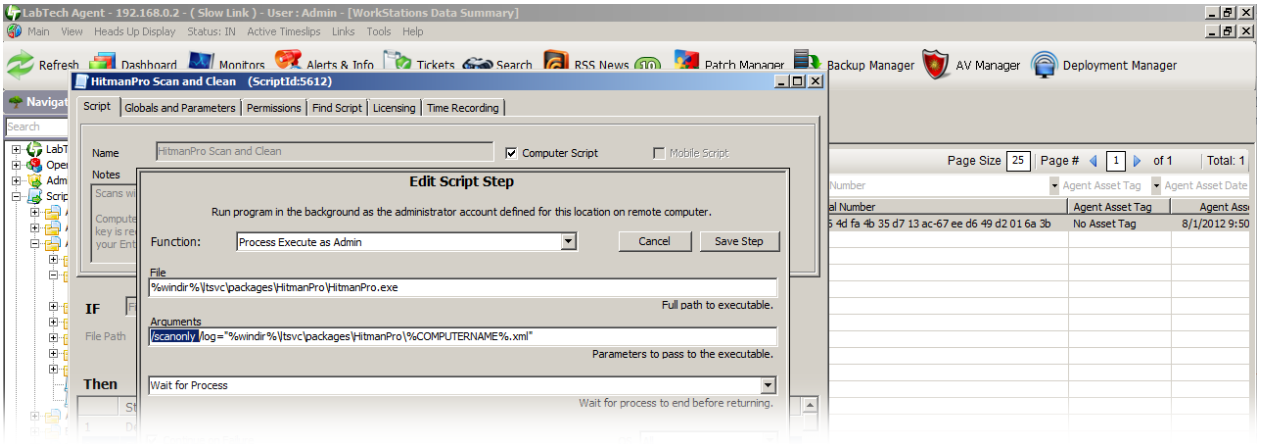
1. Download the example script: http://dl.surfright.nl/LabTech_Example.zip
2. Unpack the zip archive that contains the **HitmanPro Scan & Clean.xml** file.
3. Open the **LabTech Control Center**
4. From the **Tools** menu, select **Import > LT XML Expansion**
5. The **Browse for a File** window appears.
   Navigate to the folder that contains the **HitmanPro Scan & Clean.xml** script.
6. The **Import LabTech Expansion?** window appears. Make note of the message and click **Yes** to import the script.
7. A **LTClient** window can appear with a warning: "*Expansion contained 2 script folders, and only 0 were processed.*" Just click **OK**.
8. In the **Navigation Tree** notice the imported script in **Scripts > Anti-Virus > HitmanPro**
9. Close and restart the LabTech Control Center so the option will become available to scan computers.

Now, to scan one or more computers:

1. Open **Client Management** from e.g. the **Navigation Menu** and select the computers you wish to scan.
2. Right-click the selection and choose **Agents > Scripts > Anti-Virus > HitmanPro > HitmanPro Scan & Clean**

Scan Only

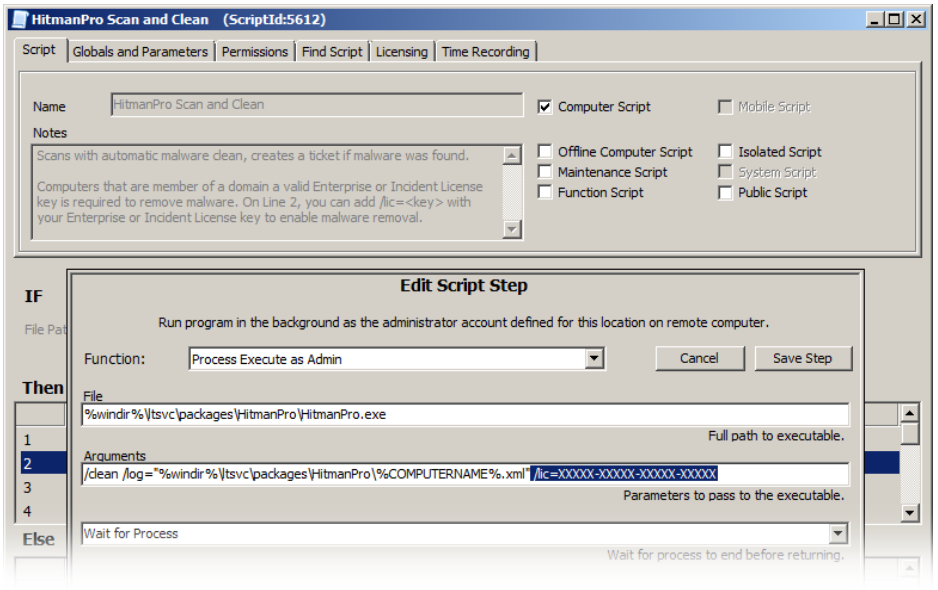
The example script will scan and remove the malware that HitmanPro encounters. You can change this behavior by opening Line 2 of **Then** and update the **Arguments** field. Replace **/clean** with **/scanonly**.



Business License

HitmanPro offers home users a free 30-day license to remove malware. Business computers on a domain are not eligible for a free license and require e.g. an Enterprise or Incident License key to enable malware removal. Note: scanning is always free for both home and businesses users, no license required.

To use your license, update the **Arguments** field on Line 2. Just add the **/lic=<key>** with your Enterprise or Incident License key to enable malware removal. For example: (replace XXXXX-XXXXX-XXXXX-XXXXX with your own key)



To purchase business licenses, visit our online shop: http://www.surfright.com/shop/business. Or sign up as a SurfRight Partner and get discounts: http://www.surfright.com/partner

Proxy Settings

HitmanPro uses by default the proxy settings from Internet Explorer which is read from the user account where HitmanPro is running under. HitmanPro additionally supports most proxy configuration options like WPAD, PAC and Manual which can be useful when running under a special account (like SYSTEM).

ProxyMode

In HitmanPro you can make proxy settings which are stored under the following registry key:

```
HKLM\Software\HitmanPro\
```

Add the value **ProxyMode** (REG_SZ) to tell HitmanPro if it should use a proxy server. Possible values:

Value	Description
(non-existing)	Proxy settings are read from Internet Explorer from the account that HitmanPro is running under.
"None"	Do not use proxy.
"WPAD"	Uses Web Proxy Auto-Discovery Protocol.
"Manual"	Registry values **ProxyPort** (REG_DWORD) and **ProxyServer** (REG_SZ) are used.
"PAC"	Registry value **ProxyPAC** (REG_SZ) specified the URL of the proxy auto configuration.

ProxyAuthentication

Additionally when **ProxyAuthentication** (REG_DWORD) is set to **1** then **ProxyUsername** (REG_SZ) and **ProxyPassword** (REG_BINARY) are used. The password is stored using AES encryption. If you want to retrieve the binary value to use in a script then you can enter the proxy password in HitmanPro once and get the value using the Windows Registry Editor (regedit.exe).

WinHTTP

You can also use the proxycfg.exe tool from Microsoft to configure the WinHTTP proxy: http://msdn.microsoft.com/en-us/library/windows/desktop/ms761351(v=vs.85).aspx

Firewall Settings

Important HitmanPro servers that you should allow in your firewall:

Host	Description
cloud.hitmanpro.nl	Malware identification servers.
activate.hitmanpro.nl	Product activation servers.
files.surfright.nl	Product update servers.

HitmanPro uses port 53, 80 and 443 (dns, http, https). All cloud communication is done over port 80 or 443 (http, https).

Command-Line Reference

The following command-line options are available in HitmanPro and particularly useful in network environments:

Option	Parameters	Meaning
`/scan`		Immediately initiates a scan of the computer and the program will be visible to the user. The EULA is automatically accepted. **Example:** `HitmanPro.exe /scan`
`/quiet`		Implies /scan but immediately initiates a silent scan of the computer. HitmanPro will be visible only in the system tray and a notification balloon is displayed, notifying the user his computer is scanned for malware. When infections are found, the program will pop up for interaction with the user. The EULA is automatically accepted. **Example:** `HitmanPro.exe /quiet`
`/scanonly`		Immediately initiates a silent scan of the computer. HitmanPro will be visible only in the system tray. Does not show a notification balloon. Program will not be installed on the local computer (implies /noinstall). The EULA is automatically accepted. **Example:** `HitmanPro.exe /scanonly`

	<file or folder>	Scan a single file or all files in a folder.
		
		Example:
		`HitmanPro.exe C:\Windows\Explorer.exe`
		`HitmanPro.exe C:\Windows\System32\`
		
		Note: The EULA is automatically accepted. Does not scan subfolders and a folder specification must end with \

`/quick`		This scan is faster than the regular scan and will only scan load point locations and in memory objects. You typically use the quick scan when you just want to check whether malware is active on the computer. **Example:** `HitmanPro.exe /scanonly /quick`

/log=	<logfile> or
	<logfile folder>
		This will instruct HitmanPro to scan a system silently and export the results to an xml log file to the specified log file folder (typically a network location). No dialogs are displayed to the user.
		
		If you specify .txt as extension, HitmanPro will export a text file instead of the default xml.
		
		Examples:
		`HitmanPro.exe /scanonly /log="Z:\%USERNAME%.txt"`
		`HitmanPro.exe /scanonly /log="Z:\%COMPUTERNAME%.xml"`
		`HitmanPro.exe /scanonly /log="\\Server\Share\Logs\"`
		
		In these examples Z: is a typical shared folder on a file server. Users (or a user group) must have the write permission on this folder and share.
		
		When specifying a folder as logfile it must end with a \
		When logging to a folder, the file name is constructed using the computer name and a date/time stamp, example:
		
		`WORKSTATION14_20100428114347.xml`

/logtype=	xml txt	Export log files in either XML or TXT format. **Example:** `HitmanPro.exe /logtype=txt /log=\\Server\Share\Logs\`
/ews		Initiate a scan of the computer with Early Warning Scoring enabled. The results xml will now also contain files that are highly suspicious but are yet unknown to our Scan Cloud. **Example:** `HitmanPro.exe /scanonly /ews`
/noupload		HitmanPro only uploads unknown but suspicious files to the Scan Cloud for virus scanning by our Malware Analysis systems and our AV partners. If you do not wish to upload any files to the Scan Cloud (because of privacy issues or government policies) you can specify this command-line option. **Example:** `HitmanPro.exe /scanonly /noupload /log="Z:\ThreatLogs\"` Note: The /noupload option will cripple the identification of unique, zero-day or early-life malware.

/excludelist=	<text file>	Exclude files and folders from the scan. The contents of the exclude list text file can be either files or folders (full paths) separated by line-feeds. Supported encoding: ANSI, UTF-8, UTF-16 and UTF-16 without BOM. **Example:** `HitmanPro.exe /scan /excludelist="Z:\excludelist.txt"`
/noupdate		Disable automatic update of the HitmanPro program. **Example:** `HitmanPro.exe /scanonly /noupdate /log="Z:\ThreatLogs\"`
/noinstall		Disable copying of the HitmanPro program to the local computer. Disables creation of shortcuts on the local computer. **Example:** `HitmanPro.exe /scan /noinstall`
/nostartboot		Disables the installation of the scan at startup component on the local computer. **Example:** `HitmanPro.exe /scan /nostartboot`
/nostartmenushortcut		Disables the creation of the Start menu folder and shortcuts. **Example:** `HitmanPro.exe /scan /nostartmenushortcut`
/nodesktopshortcut		Disables the creation of the shortcut to the HitmanPro program on the desktop. **Example:** `HitmanPro.exe /scan /nodesktopshortcut`
/noremnants		Overrides and skips the scanning and detection of remnant malware objects. Remnants are files and registry objects that once belonged to a malware infection, but this malware is no longer active on the system. This switch also disables the scanning of potentially unwanted programs (PUPs) since this also relies on the remnant scan technology. **Example:** `HitmanPro.exe /scan /noremnants`

/nopups		Overrides and skips the scanning and detection of potentially unwanted programs (PUPs). PUPs are applications that are somewhat deceitfully installed with other software you installed on the computer. E.g. the Ask toolbar is a potentially unwanted program because it is by default installed when you update your Java Runtime Environment.
/nocookies		Overrides and skips the scanning and detection of tracking cookies. **Example:** `HitmanPro.exe /scan /nocookies`
/lic=	<product key>	Automatically activate HitmanPro for the user with the supplied product key. **Example:** `HitmanPro.exe /lic=01234-ABCDE-56789-F0123 /scanonly`
/deactivate		Uninstalls HitmanPro and removes the license information from the computer.
/uninstall		Uninstalls HitmanPro but leaves the license information on the computer.
/clean		Automatically quarantine verified malicious files. Implies /scan and /noupdate. If /lic= is not specified it will automatically activate a trial or an embedded license (when allowed and applicable). **Example:** `HitmanPro.exe /clean /quiet`
/fb		Starts HitmanPro in Force Breach mode, which will terminate all non-essential processes – including malware that stops other programs from starting). **Example:** `HitmanPro.exe /fb /scan`
/renew		Reactivate the existing license to update e.g. the license duration after your Enterprise or Incident license has been extended. **Example:** `HitmanPro.exe /renew /clean /quiet`

/sr=	<file>	For experts only! Replaces the first 2 bytes of a file on the disk with SR. This will render a PE file useless. **Example:** `HitmanPro.exe /sr=C:\Windows\driver\malw.sys` Note: This is a raw write and should only be used on non-critical malicious files.

Revision History

Version	Author	Remarks
1.9	ML	Added /excludelist= switch
1.8	ML	Updated HitmanPro36.exe to HitmanPro.exe, added /uninstall switch
1.7	ML	Added /logtype, /deactivate and /nopups switches
1.6	ML	Added an example for LabTech
1.5	ML	Added Proxy Settings, Firewall Settings, /fb and /renew switch
1.4	ML	Added /clean, /noremnants and /nocookies switches
1.3	ML	Added /nostartboot, /nostartmenushortcut and /nodesktopshortcut switches
1.2	ML	Added /lic= switch
1.1	ML	Added an example for Windows Server 2008 R2
1.0	ML	Initial release