



## User Manual

## Table of Contents

1	Introduction to HitmanPro.Kickstart .....	3
2	What is ransomware? .....	4
3	Why do I need HitmanPro.Kickstart? .....	6
4	Creating a HitmanPro.Kickstart USB flash drive .....	7
5	Removing ransomware using the HitmanPro.Kickstart USB flash drive .....	11
5.1	Example ransomware removal .....	15
6	Updating the files on the USB flash drive .....	20
6.1	Adding your own files to the stick .....	20
7	Comparison .....	21

## 1 Introduction to HitmanPro.Kickstart

This document describes how HitmanPro.Kickstart can be used to rescue a ransomed PC. The intended audience ranges from non-technical users confronted with an inaccessible desktop, to support employees needing a tool to remove malware from ransomed PCs.

The intention of this document is to describe how easy it is to create a HitmanPro.Kickstart USB flash drive, and how it can be used to rescue a ransomed PC.

HitmanPro.Kickstart lets you start your computer from a USB flash drive to remove malware that has ransomed (locked) your computer and does not allow you to access it.

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

## 2 What is ransomware?

Let's first describe what ransomware does. The following description is from the Europol website<sup>1</sup>.

*A ransomware attack typically poses as a pop-up window on your screen, claiming to come from a law enforcement agency, and accuses the user of visiting illegal websites. The screen is frozen, and the message reads that it will be unlocked only on payment of a fine. Demands are very often specific to the country of the victim, pretending to be issued by local law enforcement agencies and written in the local language. Despite payment of the fine, however, the computer will not be able to be unlocked until the machine is successfully disinfected.*

*This type of attack was first detected in 2011 and has affected thousands of innocent citizens.*

*Ransomware is big business, generating millions of euros for organized criminal groups. This money is then used to finance further criminal activities all over the world. Combatting this kind of malicious software not only enables citizens to browse the Internet more safely, but also helps in the fight against organized crime.*

So essentially, when your PC has been infected with ransomware you will see a message, supposedly from the police, FBI or other authorities, demanding that a fine must be paid to unlock the computer. Most of the time, your desktop is no longer accessible and you cannot start any other program. See Figure 1 for examples of ransomware screenshots.

---

<sup>1</sup> <https://www.europol.europa.eu/content/news/%EF%BB%BF-europol-hosts-expert-meeting-combat-spread-police-ransomware-1583>

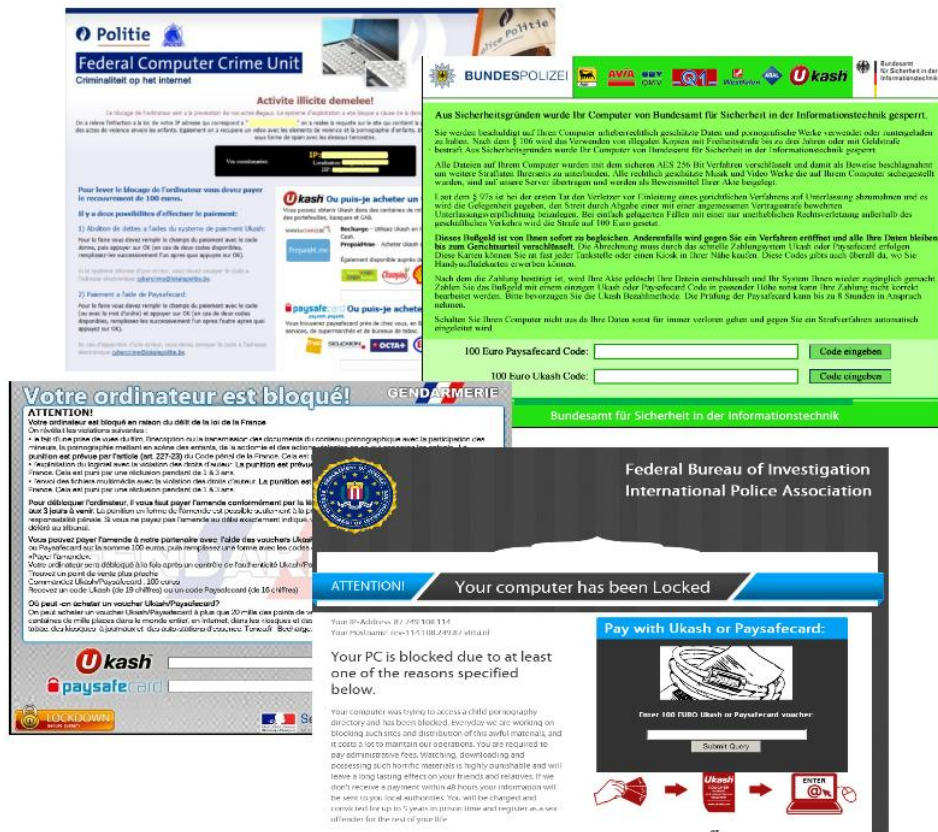


Figure 1 : Examples of ransomware

### 3 Why do I need HitmanPro.Kickstart?

Once ransomware has become active on your system, it pops up every time you restart your system and blocks access to your desktop. There is no way to start your antivirus program, or any other program, to try and remove this nasty piece of software. So how do you get rid of the malware?

There are multiple boot-CDs or rescue CDs that can be used to try to remove the malware from your system, but they all boot into an environment that is not your usual one. For instance there are rescue CDs that boot a Linux variant and offer you specialized tools to scan your disk. However, for most non-technical people, using these CDs is too difficult and may cause damaged Windows systems if the user does something wrong.

That's why we developed HitmanPro.Kickstart. It is designed to be easy to use for non-technical people without making sacrifices to the power of the HitmanPro anti-malware solution. All you need to do is boot up your system using the HitmanPro.Kickstart USB flash drive and you're ready to go. The programs on the flash drive will ensure that you boot into your own familiar Windows environment and start HitmanPro there. All the required drivers for your devices and all wireless network passwords (who can remember them?) will be readily available. There is no need to become familiar with the tools of another operating system, for instance Linux. Also, you do not have to perform manual actions like editing the registry that may cause your Windows system to become unbootable. For a more elaborate feature comparison between HitmanPro.Kickstart and currently available rescue CDs, see section 7.

## 4 Creating a HitmanPro.Kickstart USB flash drive

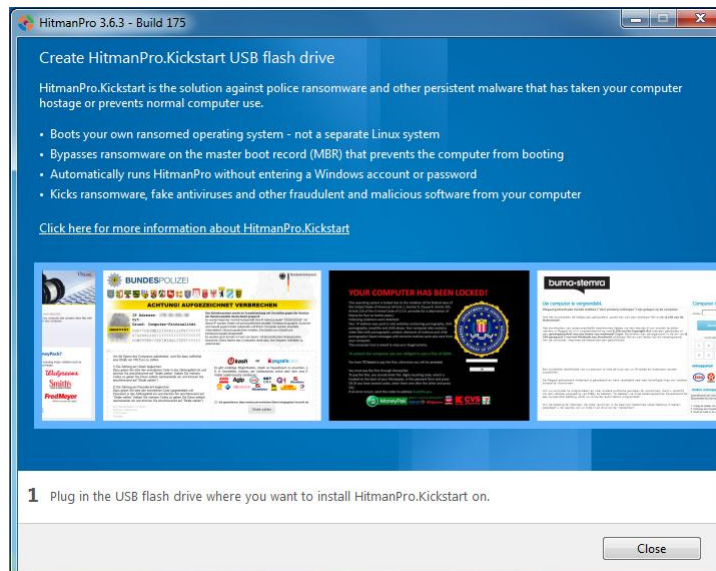
To create a HitmanPro.Kickstart USB flash drive you need to have access to a computer allowing you to start HitmanPro; you also need a USB flash drive with a capacity of at least 32Mbytes. Note: the contents of the USB flash drive will be erased during the creation process.

First, start HitmanPro. You will see a screen similar to the one shown in Figure 2.



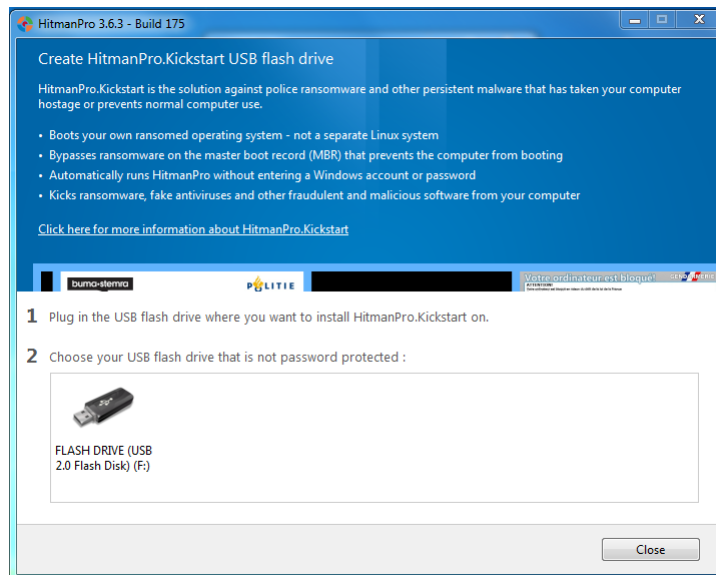
**Figure 2: HitmanPro main window**

Press the Kickstart button. A screen as shown in Figure 3 will be presented.



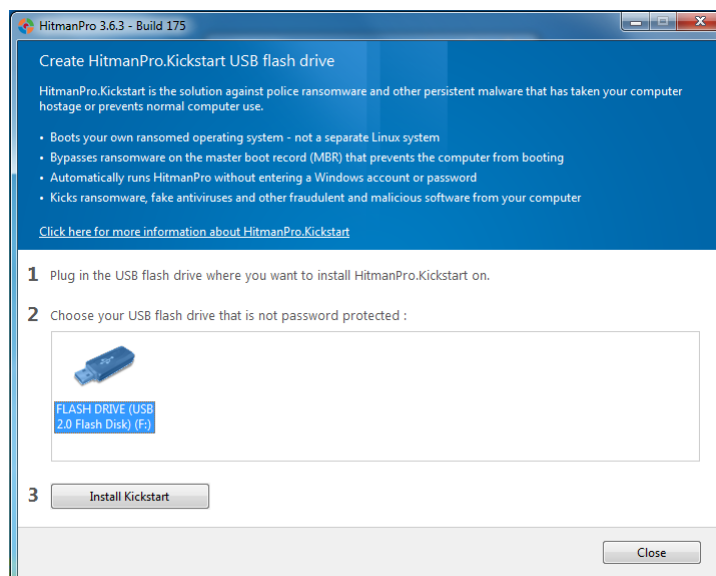
**Figure 3 : Starting the HitmanPro.Kickstart creation**

Now insert the USB flash drive you are using to write the HitmanPro.Kickstart files to. As soon as one or more USB flash drives are detected, a selection screen as shown in Figure 4 will be presented. All available target USB flash drives will be shown on this screen.



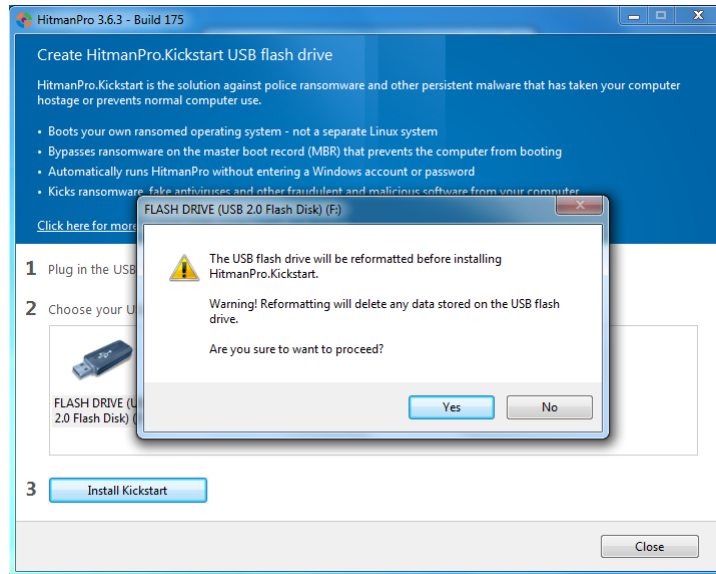
**Figure 4 : Target USB flash drive selection**

Now select the USB flash drive on which you want to place the HitmanPro.Kickstart files and press the 'Install Kickstart' button, as shown in Figure 5.



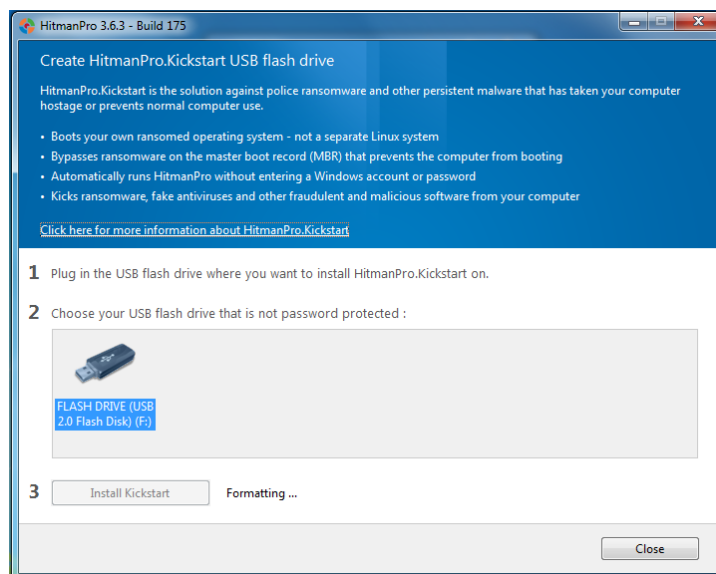
**Figure 5 : Target USB flash drive selected**

A warning as shown in Figure 6 will be presented, indicating that all contents of the selected flash drive will be erased before the HitmanPro.Kickstart files are written.



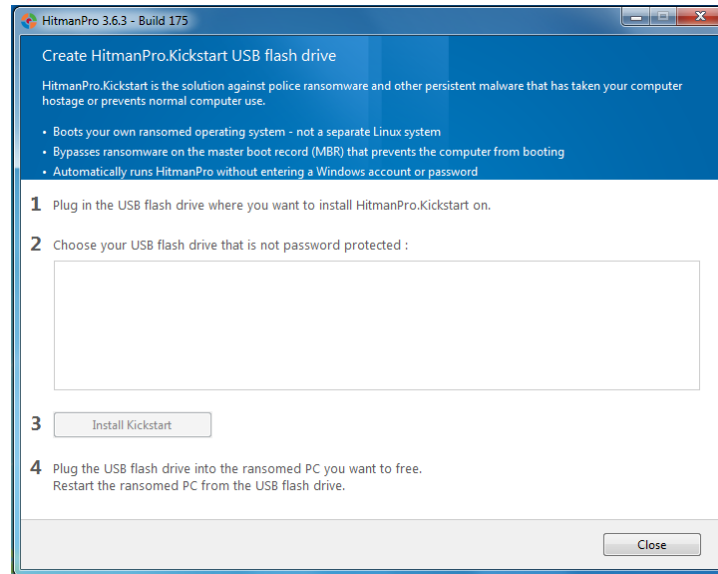
**Figure 6 : Warning message before formatting USB flash drive**

If you press the 'Yes' button now, the selected USB flash drive will be formatted and all necessary HitmanPro.Kickstart files will be retrieved from the HitmanPro servers and written to the flash drive. A progress indication is shown on the screen. See Figure 7 for an example of this progress indication.



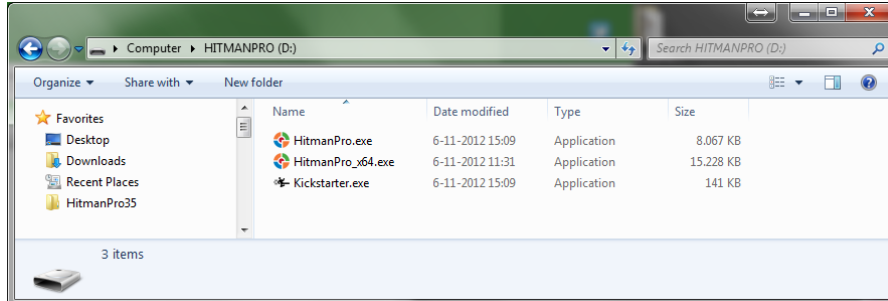
**Figure 7 : Progress indication**

Once the process has been completed a screen will be presented as shown in Figure 8. You can now remove the USB flash drive from the PC and use it to remove the malware from a ransomed PC.



**Figure 8 : HitmanPro.Kickstart USB stick creation completed**

Figure 9 shows the contents of a freshly created HitmanPro.Kickstart USB flash drive.



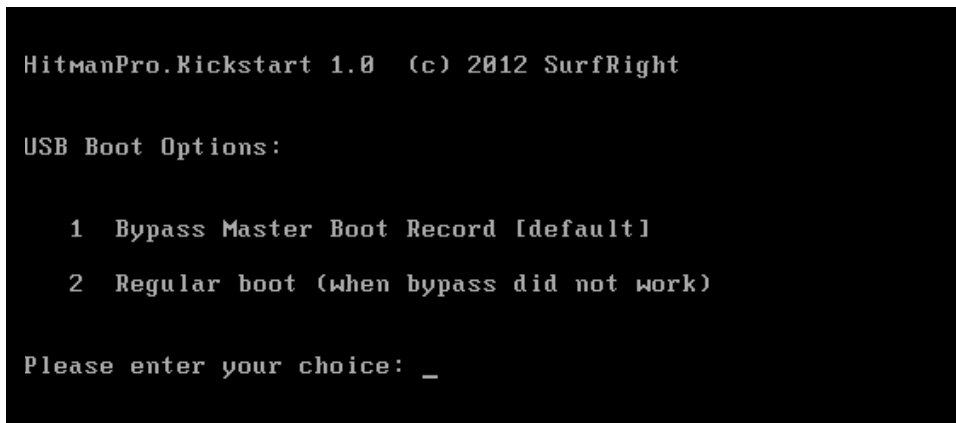
**Figure 9 : HitmanPro.Kickstart USB flash drive contents**

## 5 Removing ransomware using the HitmanPro.Kickstart USB flash drive

Once you have created a HitmanPro.Kickstart USB flash drive you can use it to rescue a ransomed PC. For that you must first make sure that the ransomed PC is powered off.

Now insert the HitmanPro.Kickstart USB flash drive into a USB port of the ransomed PC and turn on the power of the PC. During the PC's startup, enter the bootmenu of your BIOS and select the USB flash drive that contains HitmanPro.Kickstart to boot from. Note: to enter the bootmenu of your BIOS you usually have to press either F8, F11 or F12 depending on the manufacturer of your BIOS.

Once you have selected the USB flash drive to boot from and pressed the enter key, you will get the following message.



```
HitmanPro.Kickstart 1.0 (c) 2012 SurfRight

USB Boot Options:

  1 Bypass Master Boot Record [default]
  2 Regular boot (when bypass did not work)

Please enter your choice: _
```

**Figure 10 : HitmanPro.Kickstart bootmenu**

You can now enter '1' or '2' to continue booting from the hard drive. The default way to boot is '1', which skips the master boot record of your hard drive. If you do not press any key, the process will continue after 10 seconds using the default boot selection.

Option '2' should be used if you have a custom bootloader installed on your hard drive that is located in the master boot record, for instance GRUB.

If the process continues using the boot method '1', the message as shown in Figure 11 will be displayed.

```
HitmanPro.Kickstart 1.0 (c) 2012 SurfRight

USB Boot Options:

    1 Bypass Master Boot Record [default]
    2 Regular boot (when bypass did not work)

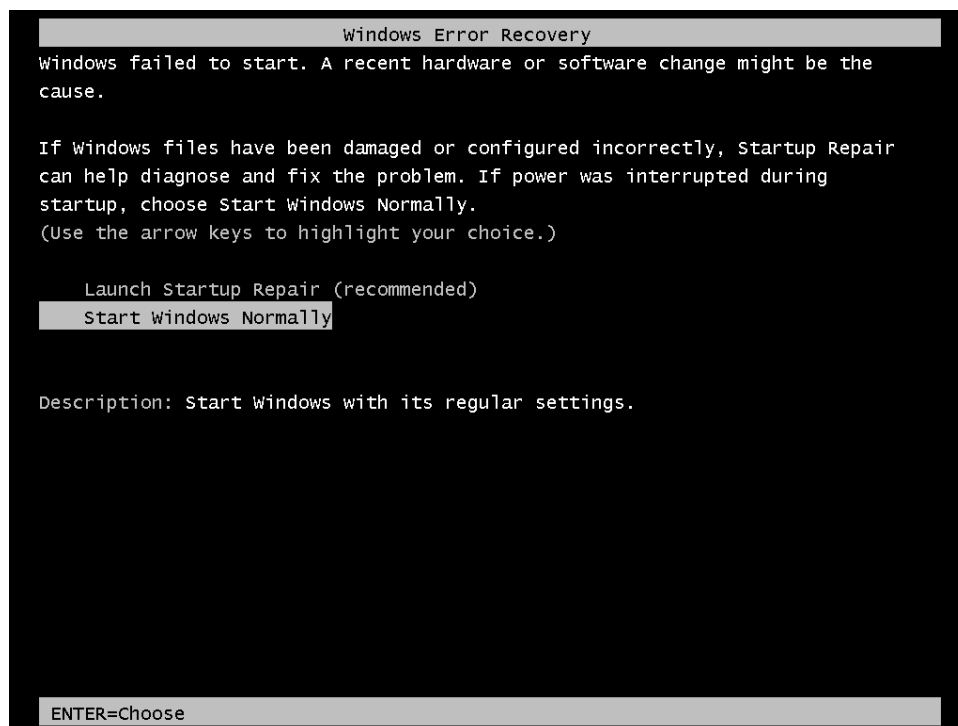
Please enter your choice: 1

HitmanPro.Kickstart booting
MBR Read
—
```

**Figure 11 : Default boot method**

After 3 seconds the system will continue booting from your hard drive and start your installation of Windows.

If you get a message like Figure 12, just choose 'Start Windows Normally'. The reason this message is displayed is sometimes because your Windows session did not shut down correctly the last time. This has no effect on HitmanPro.Kickstart.



**Figure 12 : Windows Error Recovery message**

When Windows has booted you will either get a logon screen similar to the one shown in Figure 13, or if your system is configured to logon automatically, your desktop will be started.



**Figure 13 : Windows logon with multiple users**

If you see a logon screen similar to the one shown in Figure 13 you can either select a user and logon, or if you wait approximately 15 seconds, HitmanPro will be started on your Windows logon screen as shown in Figure 14.



**Figure 14 : HitmanPro started on logon screen**

If you selected a user, the environment of that user will be started and HitmanPro will be started in that environment, see Figure 15.



**Figure 15 : HitmanPro started on user's desktop**

Note: For the removal of ransomware it makes no difference if HitmanPro is started on the logon screen or if it is started in a user environment.

Once HitmanPro has started you can press 'Next' to start the scan and if malware is found, remove it.

## 5.1 Example ransomware removal

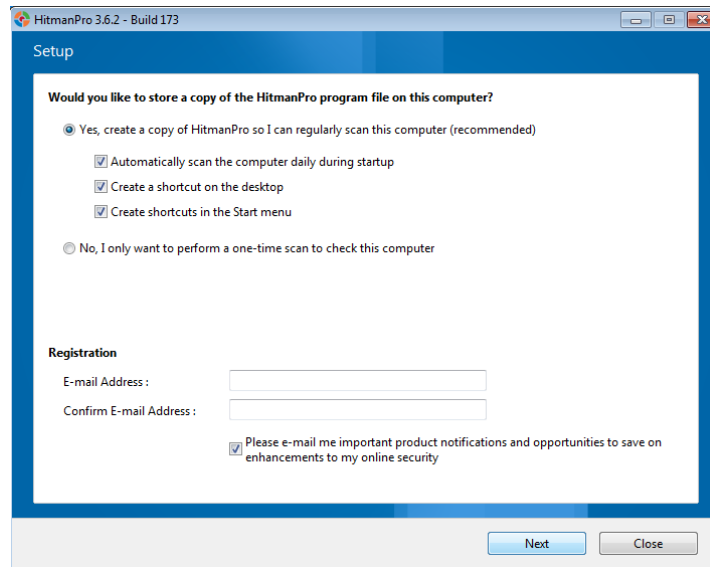
Now let's demonstrate the removal of ransomware using the following example where a PC is ransomed by Moneypack ransomware as shown in Figure 16.



Figure 16 : Moneypack ransomware

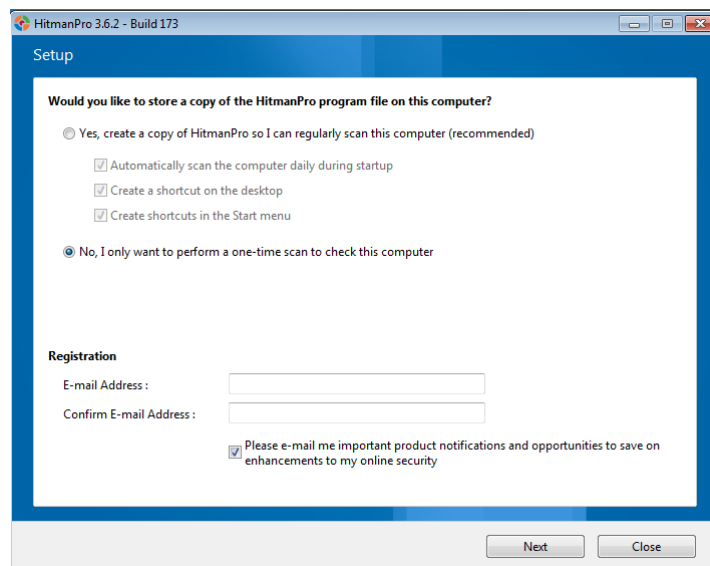
Once the PC has booted, following the procedure described in section 5 'Removing ransomware using the HitmanPro.Kickstart USB flash drive', you will see the HitmanPro start screen similar to Figure 14 or Figure 15.

Now press the 'Next' button to start scanning for malware. If this is the first time HitmanPro has started on this machine, you will see a screen as shown in Figure 17.



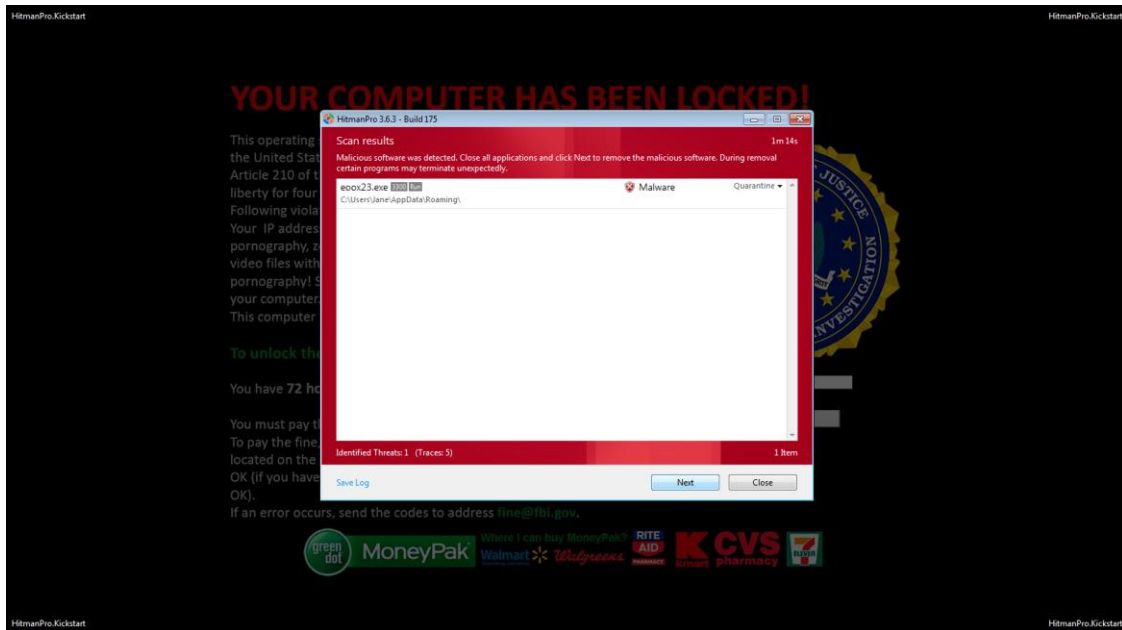
**Figure 17 : HitmanPro install window**

On this screen you can select whether you want to install HitmanPro on this PC or if you want to scan this machine without installing the software to your hard disk (Figure 18).



**Figure 18 : Start without installing to local hard disk**

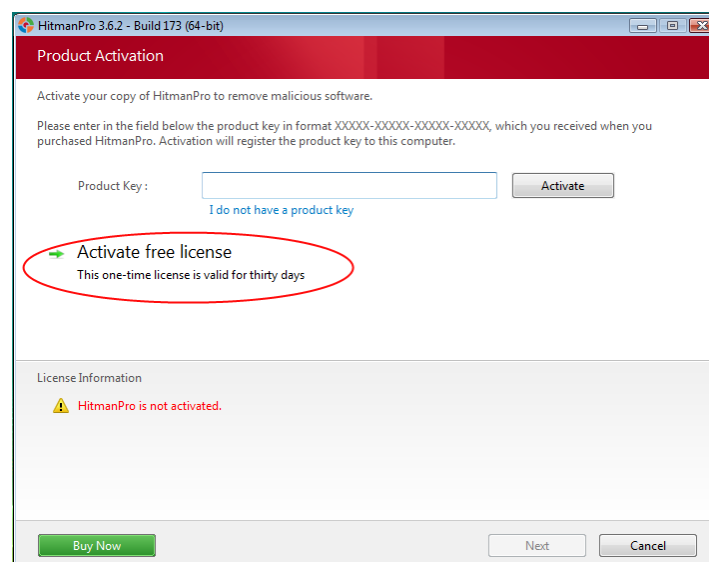
If you press the 'Next' button, system scanning will begin and if malware is detected, a screen as shown in Figure 19 will be shown, indicating what malware is present on your system.



**Figure 19 : Malware detected**

You can now select the 'Next' button to quarantine the malware. In this way, the malware is moved into a secure store and can no longer start.

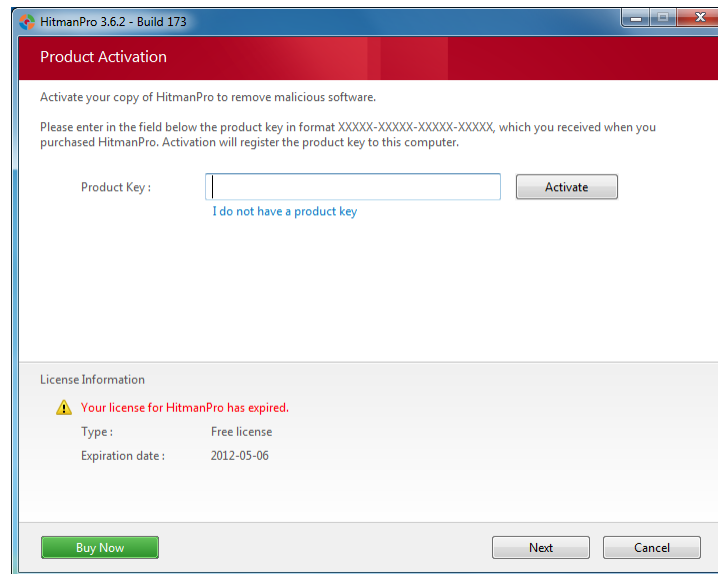
If you are a home user, and there is no valid license present on your system, and this machine has also never used the free HitmanPro trial license, then you will see a screen as shown in Figure 20. Here you can either activate the 30-day free license or you can enter the product key you have purchased.



**Figure 20 : Activate free trial**

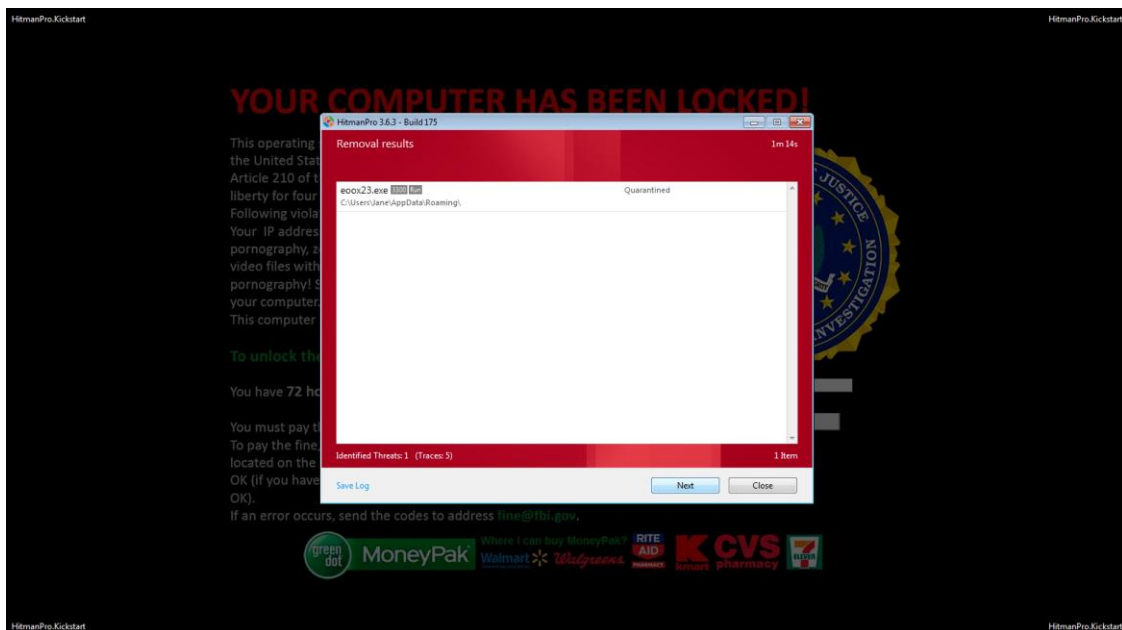
If the system you want to rescue had already used a HitmanPro free license previously, and this license has expired, or your computer is used in a business environment, you will see a screen as shown in

Figure 21. To be able to remove the malware you need to enter a valid product key that you have purchased.



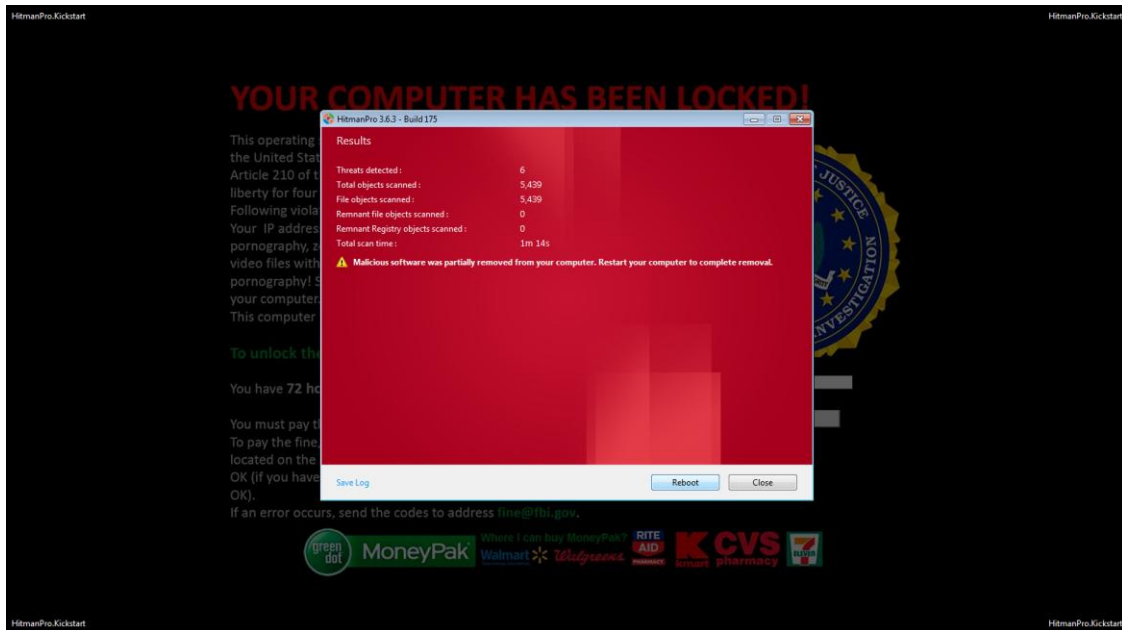
**Figure 21 : Trial expired**

Once HitmanPro has been activated successfully, the removal process will continue if you press the 'Next' button. After some time you will see a screen similar to Figure 22, indicating that the malware has been successfully disabled or removed.



**Figure 22 : Malware quarantined**

The malware removal process is now finished. If you press 'Next' you will see a screen as shown in Figure 23.



**Figure 23 : Malware removed, reboot required**

Now remove the USB flash drive and press the 'Close' or 'Reboot' button. Either of them will cause the PC to reboot.

After the PC has rebooted, your PC will be free of ransomware. It is advised that you perform another scan with HitmanPro to verify that all malware has been removed from your PC.

## 6 Updating the files on the USB flash drive

The HitmanPro application is improved actively, and new versions are released on a regular basis. To be able to use these new versions with the HitmanPro.Kickstart USB flash drive you need to put these new versions on the flash drive.

You can download the new version of HitmanPro from our website, [www.surfright.com](http://www.surfright.com) and copy the file to the USB flash drive. Note that the filename **must** be either HitmanPro.exe or HitmanPro\_x64.exe. See Figure 24 for an example of the files and their names on the USB flash drive.

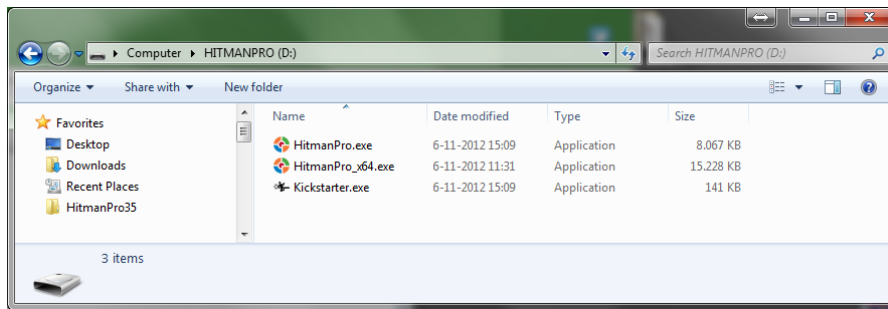


Figure 24 : HitmanPro.Kickstart USB flash drive contents

Alternatively you can start the HitmanPro application in a non-ransomed Windows environment directly from the USB flash drive. If a new version of HitmanPro is available, it will be updated on your flash drive automatically. Note: if HitmanPro.Kickstart is used to boot a ransomed PC, the HitmanPro application on your flash drive will **not** be updated automatically.

### 6.1 Adding your own files to the stick

You can add your own files to the stick if you like. This way you can still use all the remaining space that is left on your USB flash drive once you have turned it into a HitmanPro.Kickstart flash drive. Just as long as you leave the files *HitmanPro.exe*, *HitmanPro\_x64.exe* and *Kickstarter.exe* on the flash drive, adding your own files to the contents of the drive will not interfere with the HitmanPro.Kickstart functionality.

## 7 Comparison

The following table lists a number of HitmanPro.Kickstart's features and compares them to currently available rescue CD's.

Feature	Rescue CD	HitmanPro.Kickstart
Free product	✓	✓
Easy to use by non-technical computer user	✗	✓
Bypasses Master Boot Record (Sector 0) bootkits	✓	✓
Uses multiple anti-virus engines	✓ <sup>1</sup>	✓
Zero-day detection using behavioral scan	✗	✓
No need for virus definition updates	✗	✓
Fast scan takes less than 5 minutes (on average)	✗	✓
Access the internet without having to enter your Wi-Fi network credentials <sup>2</sup>	✗	✓
Uses the Windows drivers that are needed for your specific hardware <sup>3</sup> , no matter how old or exotic your system is	✗	✓
Creates restore point to revert changes	✗	✓
Replaces infected system files with clean versions	✗	✓
Creation of bootable medium integrated in single application	✗	✓
Sustainable – updatable medium	✗	✓
Full-fledged product instead of trimmed antivirus subset	✗	✓

<sup>1</sup> Some rescue CDs do combine multiple antivirus engines – most rescue CDs do not.

<sup>2</sup> Kickstart boots your Microsoft Windows environment which already had access to your Wi-Fi network.

<sup>3</sup> Not all your hardware may be supported by a Linux environment.

## Revision History

Version	Author	Remarks
1.0	EE	Initial release