TROJAN KILLER
REVIEW OF ANTIMALWARE SOFTWARE
BY
UKRAINIAN GRIDINSOFT LCC

NOVEMBER 2014

AV LAB
THE INDEPENDENT ANTIVIRUS TESTS

Trojan Killer – review of antimalware software by Ukrainian GridinSoft LCC

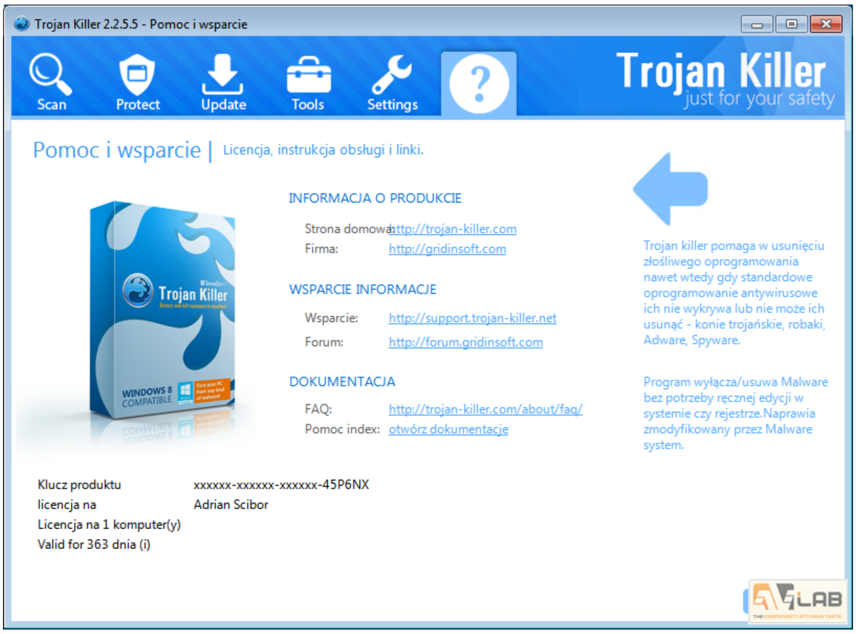
Trojan Killer software created by the Ukrainian GridinSoft LLC company is make for removing malware from infected computers even if antivirus software isn't able to detect it. In principle, Trojan Killer deals with various types of threats ranging from adware, spyware, worms to trojan horses. What is its efficiency? We checked it out in our test show below. Program removes effects of threats in files as well as in registry entries added by malicious software.

About GridinSoft LLC

GridinSoft LLC was founded in 2003 in town of Kremenchuk. At the very beginning, the company had only one employee, who was rudder, sail and ship of whole business. With time, custom made applications gathered around it new crew members. Newly formed group began to develop its own software. In particular they were text and graphics editors one of which became very popular among employees of large global corporations such as Microsoft, Toshiba and Philips – we are referring to **CridinSoft CHM Editor**. Thanks to the success of this application, team decided to continue to develop programs to wider range of users.

The beginnings of Trojan Killer

In early 2000, antivirus software available on the market didn't guarantee 100 percent computer protection and that led to appear new antimalware programs. Then Trojan Killer was born and GridinSoft LLC has become a profitable antivirus company, which currently protects thousands of users around the world. Today the software has been downloaded over a million times and it's estimated that it removed 5 million threats.



Trojan Killer 2.2.5.5 - Pomoc i wsparcie

Pomoc i wsparcie | Licencja, instrukcja obsługi i linki.

INFORMACJA O PRODUKCIE

Strona domowa: http://trojan-killer.com
Firma: http://gridinsoft.com

WSPARCIE INFORMACJE

Wsparcie: http://support.trojan-killer.net
Forum: http://forum.gridinsoft.com

DOKUMENTACJA

FAQ: http://trojan-killer.com/about/faq/
Pomoc index: otwórz dokumentacje

Trojan killer pomaga w usunięciu złośliwego oprogramowania nawet wtedy gdy standardowe oprogramowanie antywirusowe ich nie wykrywa lub nie może ich usunąć - konie trojańskie, robaki, Adware, Spyware.

Program wyłącza/usuwa Malware bez potrzeby ręcznej edycji w systemie czy rejestrze.Naprawia zmodyfikowany przez Malware system.

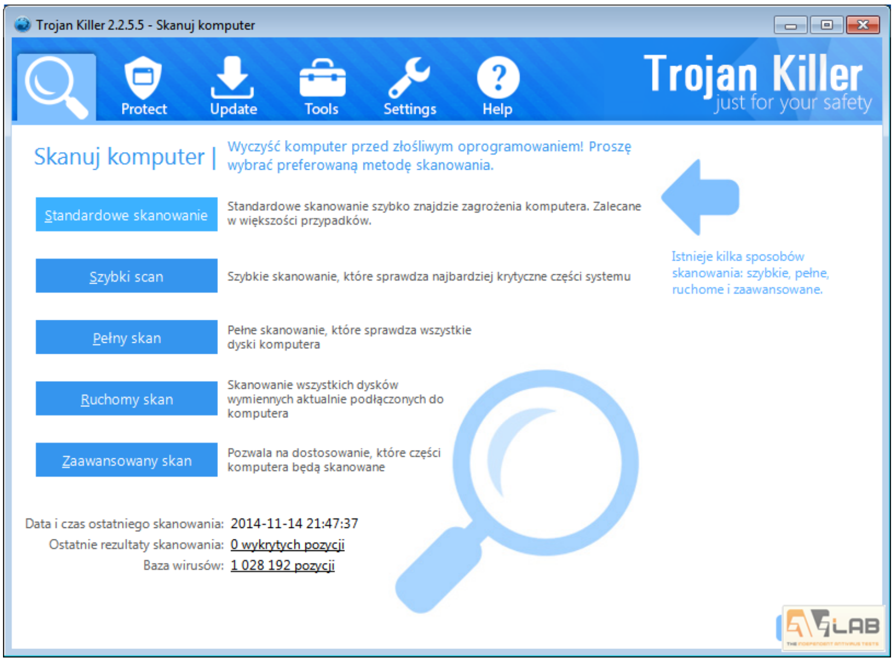
Klucz produktu	xxxxxx-xxxxxx-xxxxxx-45P6NX
licencja na	Adrian Scibor
Licencja na 1 komputer(y)	
Valid for 363 dnia (i)	

Rysunek 1 Information about Trojan Killer

Trojan Killer is assumed to be on-demand scanner, it also has real-time protection module, which is disabled by default. The application is based on an original antivirus engine, which doesn't use any third party technology. Software removes threat from system when it's detected during scanning process. Due to high diversity as well as quick generic reproduction of all kinds of web threats, Trojan Killer uses heuristic algorithms designed to provide better protection against unknown threats, especially the latest malware mutation. Trojan Killer also uses standard virus database which contains approximately 1 145 000 items.

The basic function – scanning

Basic Trojan Killer module is malware scanner, which permanently removes threat after it is detected on user computer.



Skanuj komputer | Wyczyść komputer przed złośliwym oprogramowaniem! Proszę wybrać preferowaną metodę skanowania.

Standardowe skanowanie szybko znajdzie zagrożenia komputera. Zalecane w większości przypadków.

Szybkie skanowanie, które sprawdza najbardziej krytyczne części systemu

Pełne skanowanie, które sprawdza wszystkie dyski komputera

Skanowanie wszystkich dysków wymiennych aktualnie podłączonych do komputera

Pozwala na dostosowanie, które części komputera będą skanowane

Istnieje kilka sposobów skanowania: szybkie, pełne, ruchome i zaawansowane.

Data i czas ostatniego skanowania: 2014-11-14 21:47:37
Ostatnie rezultaty skanowania: 0 wykrytych pozycji
Baza wirusów: 1 028 192 pozycji

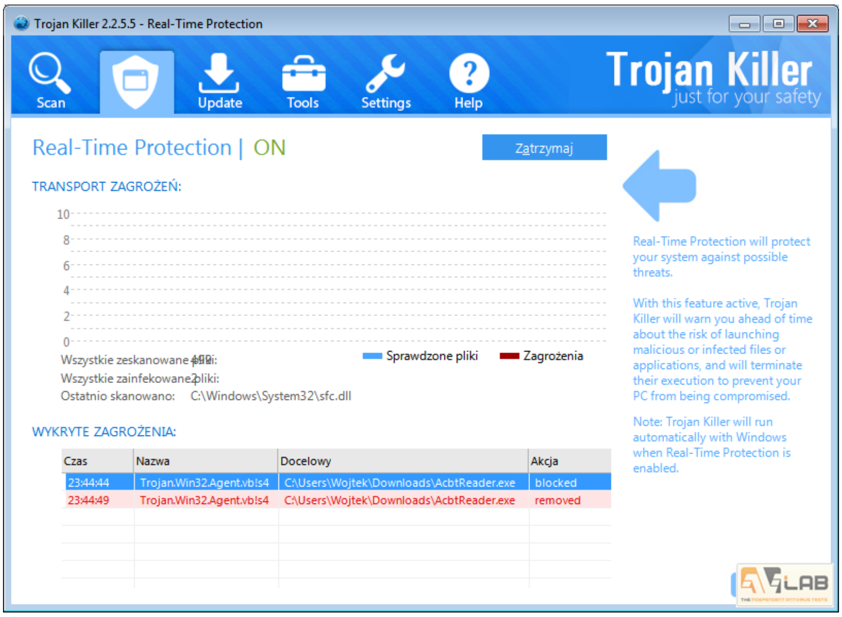
Rysunek 2 Computer Scanning

Program allows to perform different kinds of scanning:

- Standard scan is automatically activated after software is started
- Quick scan checks the most critical part of the system
- Full scan searches all computer disks, it's long process, but it gives the highest level of protection
- Removable scan allows to scan removable drives connected to the computer
- Custom scan allows user to define, which parts of the system should be scanned, including folders, files, partition.

Real-time protection

Trojan Killer has real-time protection module, which is disabled by default. But after it starts, when Trojan Killer works in the background scanning for threats all files on regular basis, we can feel protected. In case of malware detection, we are informed about it immediately and software blocks its activity. User can add infected file to the quarantine or ignore threat, but it isn't recommended unless user is sure about harmlessness of a file.



Real-Time Protection | ON

TRANSPORT ZAGROŻEŃ:

Wszystkie zeskanowane [illegible] pliki:
Wszystkie zainfekowane 2 pliki:
Ostatnio skanowano: C:\Windows\System32\sfc.dll

WYKRYTE ZAGROŻENIA:

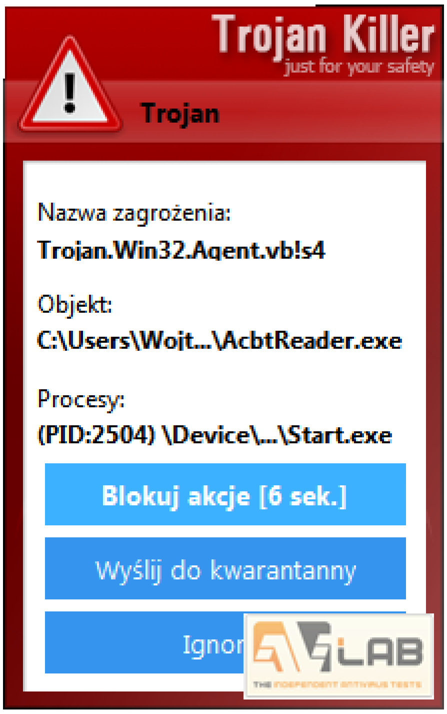
Czas	Nazwa	Docelowy	Akcja
23:44:44	Trojan.Win32.Agent.vb!s4	C:\Users\Wojtek\Downloads\AcbtReader.exe	blocked
23:44:49	Trojan.Win32.Agent.vb!s4	C:\Users\Wojtek\Downloads\AcbtReader.exe	removed

Real-Time Protection will protect your system against possible threats.

With this feature active, Trojan Killer will warn you ahead of time about the risk of launching malicious or infected files or applications, and will terminate their execution to prevent your PC from being compromised.

Note: Trojan Killer will run automatically with Windows when Real-Time Protection is enabled.

Rysunek 3 Real-time protection – disabled by default



Nazwa zagrożenia:
Trojan.Win32.Agent.vb!s4

Objekt:
C:\Users\Wojt...\AcbtReader.exe

Procesy:
(PID:2504) \Device\...\Start.exe

Rysunek 4 Message with information about found threat

Additional tools

- **Resetting browser settings**

Some threats (adware) can change web browser default settings, for example default home page. Trojan Killer allows user to restore any modification (home page, search engines, unwanted add-ons) to its original state in all popular web browsers (Internet Explorer, Google Chrome, Mozilla Firefox, Opera). It is also able to reset HOSTS file, proxy settings for Internet Explorer and clear DNS cache.

- **Resetting rules for updating**

Some malware block Windows Update service responsible for installing updates in operating system and limit settings on the configuration screen. This option unlocks modifications made by malware.

- **Others**

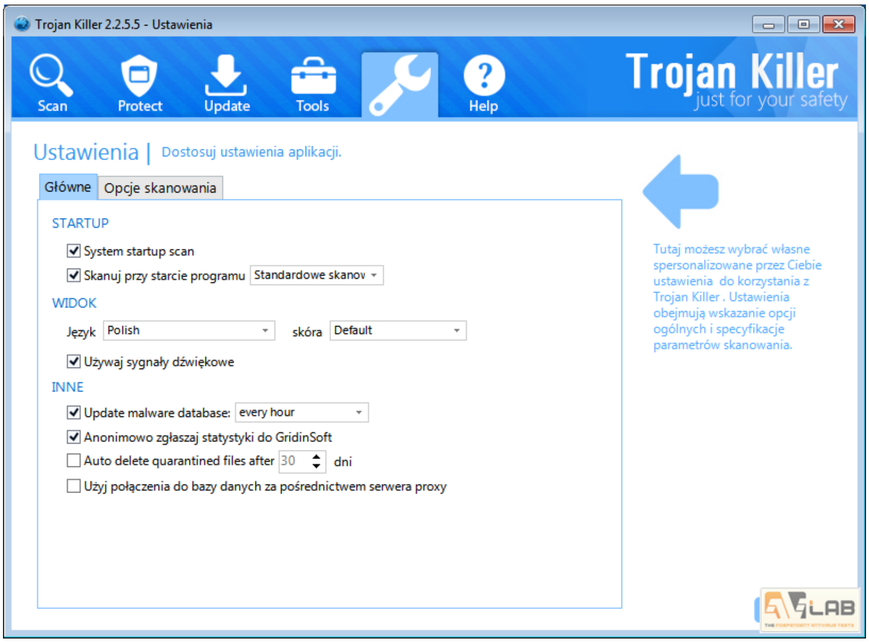
From available tools we also have possibility to create list of files and folders that you want to ignore during scanning. Program saves and archives all files with scan results performed on the computer. There is also possibility to view quarantine and restore, copy or deleted files located in it.

- **Information about system**

This module allows user to generate log file that contains information about configuration and functionality of the system, including running services, active processes and content of HOST file. We can submit a generated data to technical support, which sends us recommendation for removing threat.

Application customizing

Application allows to customize settings according to user needs. We can set scan type at system startup, change interface look, update details and language – software is also available in Polish language created by a group of enthusiast.



STARTUP

☑ System startup scan

☑ Skanuj przy starcie programu: Standardowe skanov

WIDOK

Język: Polish   skóra: Default

☑ Używaj sygnały dźwiękowe

INNE

☑ Update malware database: every hour

☑ Anonimowo zgłaszaj statystyki do GridinSoft

☐ Auto delete quarantined files after 30 dni

☐ Użyj połączenia do bazy danych za pośrednictwem serwera proxy

Tutaj możesz wybrać własne spersonalizowane przez Ciebie ustawienia do korzystania z Trojan Killer . Ustawienia obejmują wskazanie opcji ogólnych i specyfikacje parametrów skanowania.

Rysunek 5 Trojan Killer settings

In settings we can change modify scanning process enhancing its accuracy, but whole scanning process will be longer.

Tests

Methodology: Trojan Killer runs on default settings with real-time protection, Internet Explorer 11, Google Chrome 38, Windows 7 x64 Professional + SP1.

- To see effectiveness in real-time, we used 40 links to malware and test was divided into 2 parts:

Since program doesn’t provide HTTP protection, we skipped this test and phishing one as well.

We scanned threats downloaded on hard drive with on-demand scanner, which detected 34/40 threats and that is 85%. Next we checked effectiveness of proactive protection. When we run six undetected threats, program detected two of them, so 4 samples from 40 disgraced software infecting the system. **Trojan Killer detected 36/40 threats.**

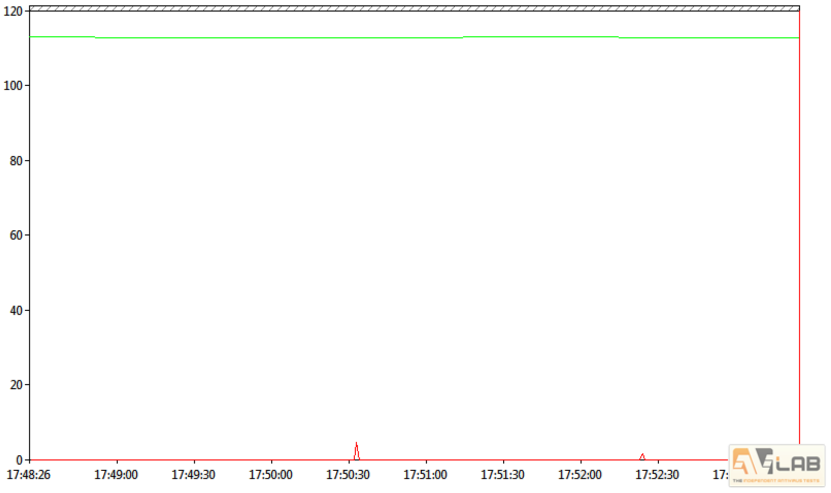
NOTES: Even enabling real-time protection and saving file on hard drive, Trojan Killer doesn’t scan it automatically, only when user runs scan manually and file turns out to be a virus, action taken by it is blocked. User is informed about the threat in message window, where he can decide to delete or ignore it. This isn’t program error. We received a response from producer, that Trojan Killer works that way.

- To check Trojan Killer static detection, we prepared 1000 samples, which consisted of adware, trojans, viruses, backdoors, worms, key loggers and other malicious software download from VirusSign. When test was performed, software ran on default settings and had access to the Internet. Test is dated 17 November 2014. Trojan Killer detected 260/1000 threats.

Performance of Trojan Killer

In order to perform performance test, we prepared virtual Windows 7 x64 Professional + SP1 with updates date 17 November. On the system we installed Adobe Reader, Google Chrome, Java, Opera and several other programs. We checked usage of processor and memory by Trojan Killer processes, on idle and during scan with default settings (we enabled real-time protection, which is disabled by default). During 5 minutes test, we were collecting data every 1 second.

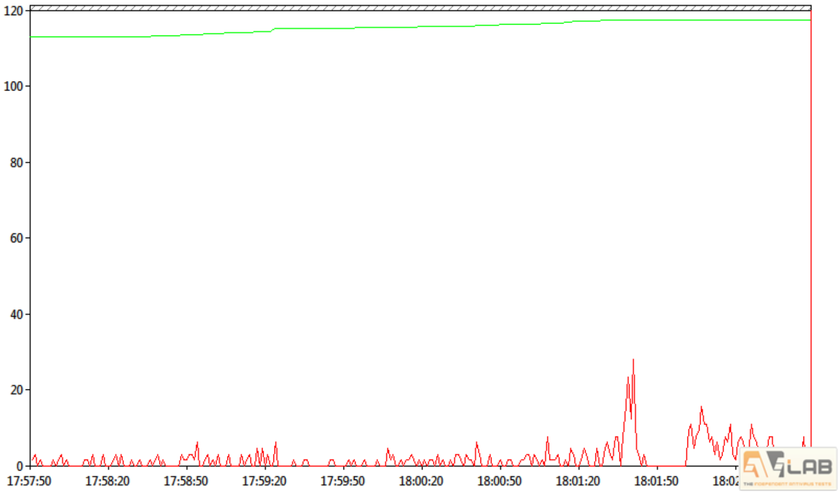
Usage of resources on idle



Average usage of resources by Trojan Killer processes during 5 minutes on idle:

CPU [%]	RAM [~MB]
0,021	108

Usage of resources during scan



Average usage of resources by Trojan Killer processes during 5 minutes of scanning

CPU [%]	RAM [~MB]
1,998	110

Summary

Trojan Killer software combines on-demand scanner with real-time protection against malware on average level. The application can only be a good complement for already installed security software, when it has a problem with removing threat. Static threats detection result of 26% isn't the best, as evidenced by our on-demand scanner test in October.

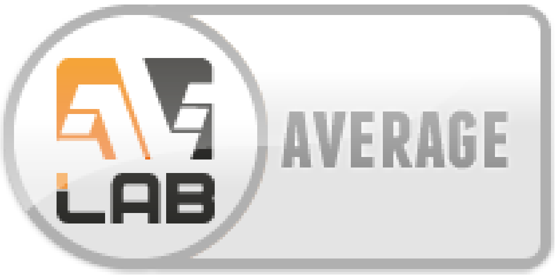
Regarding observed errors, application doesn't allow user to scan a single file. Also Polish version of the program is incomplete, some phrases are not translated very well, but producer assures us – it's created by software enthusiasts, so we forgive this mistake.

Due to its nature, software doesn't need much processor resources, but memory usage could be reduced, although we must admit that it remains at the same level – approximately 110MB.

According to the producer, Trojan Killer is continuously developed, it is planned to implement license for more computers, now one license can be used only on two computers. Producer also told us about working to implement firewall, which will increase level of protection for sure.

In summary, product being on-demand scanner with optional real-time protection, which costs approximately 160 zł/2 computers/year is definitely too high compared to possibilities of the program.

In this price or little higher, we can buy full security suite with many modules protecting more computers and mobile systems (F-Secure SAFE, ESET Smart Security Pack, McAfee LiveSafe).



15-day trial version of Trojan Killer is available at this link.

Review in Polish language is available at this webpage.