SocioBrains
ISSN 2367-5721, JOURNAL HOMEPAGE: WWW.SOCIOBRAINS.COM
INTERNATIONAL SCIENTIFIC REFEREED ONLINE JOURNAL WITH IMPACT FACTOR
ISSUE 42, FEBRUARY 2018

SOME METHODS OF PROTECTION FROM UNWANTED CONTENT

Abstract: This article reviews some of the ways for unwanted content to reach out to the internet user and the appropriate safeguards and protections for this to be countered.

Author information:

Ivailo Burov
At Konstantin Preslavsky – University of Shumen
✉ i.burov@shu.bg
Bulgaria

Keywords:
ads, adware, malware, bundling, DNS protection, local DNS mapping

При работа с приложения, имащи достъп до интернет, извеждането на нежелано съдържание се превръща във все по-голям проблем за потребителя. Съществуват спорове между рекламодателите и потребителите дали трябва да се блокира рекламното съдържание. От една страна собственици на сайтове, предлагащи безплатни услуги на потребителите като например много от новинарските, се издържат главно от средства, получавани от рекламно съдържание, но от друга страна дразнещите реклами, особено такива, несвързани с търсеното от потребителя съдържание, изскачащи прозорци или мигащи банери с ярки цветове за привличане на вниманието, правят ползването на предоставяната безплатна услуга не само дразнещо и затруднено, но в някои случаи почти невъзможно. Към това спадат включително и такива с аудио или видео съдържание, стартиращо с максимален звук. В допълнение някои некоректни рекламодатели използват специално създаван за рекламна цел софтуер (adware), посредством който заразената веднъж машина или браузър извършва препратки към сайтове с нежелано и дори порнографско съдържание. От гледна точка на потребителя, освен затормозяващо работата, нежеланото рекламно съдържание е свързано и с натоварване на системните ресурси, което е най-нежелано при използване на мобилни устройства, защото води до бързо изтощаване на батерията и намалява срока и на ползване. Във връзка с повишеното използване на ресурсите на потребителската платформа е необходимо да се спомене, че някои производители на операционни системи включват в новите си версии и ъпдейти към старите версии услуги за телеметрия, които водят не само до забавяне на системата като цяло, а и до събиране на данни за поведението на потребителя. Такива процеси не се регистрират като шпионски от антивирусните програми, но могат да доведат до значително натоварване и следователно забавяне на системата. За успешното предпазване от нежелано съдържание е необходимо познаване на основните пътища, по които то достига до потребителя. Въпреки, че настоящата статия не фокусира вниманието си към компютърната сигурност, един от основните пътища за разпространение на нежелано съдържание е свързан точно с пропуски в сигурността.

Най-често срещани методи за разпространение на рекламно съдържание

Най-често срещаните методи за разпространение на рекламно съдържание са:

- През браузъра при посещение на определена уеб страница
- През интерфейса на безплатен софтуер от типа (freeware, shareware)
- Посредством инсталиран на потребителската система рекламен софтуер, известен като адуер (adware)

Докато първите два метода се възприемат най-често като легални, въпреки множеството спорове по въпроса относно анонимност и трансфер на лични данни, използването на адуер обикновено се третира като нелегитимен начин за представяне на рекламно съдържание, независимо че разпространителите му заобиколят това, чрез упоменаване в лицензното споразумение при инсталацията на подобна особеност. В този случай се разчита на това, че потребителят не е склонен да чете дълги, написани с дребен шрифт и представени в миниатюрен прозорец лицензни споразумения за безплатен софтуер написани най-често само на английски език.

При разпространение на нежелано съдържание през браузъра при посещение на уеб страница, създателите на съответния уеб сайт осигуряват пари за поддръжка на уеб сайта си от рекламни материали на трети лица, а при разпространението му през интерфейса на безплатен софтуер от типа (freeware, shareware), авторът на безплатния софтуер генерира приходи, като представя тези материали в интерфейса на продукта си.

Разпространение на нежелано съдържание през браузъра

Съвременните браузъри разполагат с активирана по подразбиране защита срещу изскачащи прозорци и по този начин се блокира нежеланото съдържание, представяно по тази начин, но в някои случаи тя може да бъде преодоляна. Разработчиците им се придържат към изискванията за сигурност, налагана от последните уеб стандарти, като ограничават разглежданите сайтове откъм достъп за произволно четене и запис на данни в системата на потребителя, но същевременно им предоставят определени възможности за синхронизация с потребителската система, предвидени за улесняващи потребителя дейности като автоматично запомняне на потребителското име или парола (сесийни данни). Пример за това са т.н "бисквитки" (cookies), които представляват малки текстови файлчета, които уеб сайтът записва в определено място за съхранение на потребителската система, от което може да записва и чете данни. За разлика от **сесийните бисквитки**, които са свързани предимно с идентификация на потребителския профил, съществува и друга категория, известна като **трасиращи бисквитки**(tracing cookies). Те служат за колекция на данни за поведението на потребителя, неговите предпочитания, разглежданите от него продукти, а също така и данни достъпни от уеб браузъра като: използвана операционна система, резолюция на екрана, географско разположение, езикови настройки и др. Цялата тази информация може да бъде използвана от собственика на сайта или да бъде предоставяна на партньорски организации с цел представяне на определен тип рекламно съдържание. Макар, че това е подбрана според съставяния профил реклама, тя може да бъде пренасочена като пощенско съдържание към имейл адреса на потребителя известно като "спам".

С развитието на социалните мрежи почти всички сайтове, партниращи си с такива мрежи използват подобни трасиращи бисквитки, като данните биват предоставяни на съответната социална мрежа. Един илюстративен пример е посещението от потребител, неизлязъл от Фейсбук профила си на сайт, с включени в него Фейсбук услуги, като повечето новинарски сайтове: там се появява списък с профилите на неговите Фейсбук приятели харесали сайта или определена статия, при това без потребителят да е извършил регистрация към въпросния сайт. В този аспект е необходимо да се отбележи, че освен липсата на анонимност, се трансферират и лични данни през различните медии.

Друг такъв пример за трансфер на лична информация, който разчита предимно на ленивостта на потребителя, е избягването на регистрация, посредством предоставена възможност за извършване на поръчка посредством наличен потребителски профил в социална мрежа или такъв от някоя известна уеб услуга. Въпреки, че потребителят е избягнал досадното попълване на данни при извършване на поръчката, при използване на социалната мрежа в скоро започва да получава реклама, свързана със стоките и услугите, които е разглеждал във въпросния сайт - т.е. адаптирано към профила на потребителя рекламно съдържание.

Без да бъде вземана страна спрямо плюсовете и минусите на тези методи на разпространение на рекламно съдържание, презентирането на такова води до по-голям разход

на системни ресурси като процесорно време и оперативна памет, като следствията са: намалено бързодействие на системата, повишен температурен режим, по-кратко време за изразходване на батерията при мобилните устройства и др.

Ограничаване на нежеланата реклама с помощта на блокиращи разширения в браузъра

Разпространение на нежелано съдържание през интерфейса на безплатен софтуер от типа (freeware, shareware)

В основни линии това е легално разпространение на рекламно съдържание, което осигурява доходи на създателя на безплатния продукт, но напоследък се наблюдава тенденция към представяне на това съдържание в подвеждащи изскачащи прозорци или линкове, заместващи функционалния, като по този начин потребителят се подвежда към неволно пренасочване към услуга на трети лица или инсталиране на техен продукт, което до известна степен размива границата между безплатния софтуер и адуер. Особено силно това се наблюдава при безплатните мобилни приложения. Освен всички неприятни последствия, описани досега, при мобилните системи трябва да се споменат и ограниченията свързани с интернет трафика на подобни устройства. Повечето изследвания в тази област определят използвания трафик за реклама като близо две трети от общия трафик, използван от потребителя. В такъв случай в зависимост от договора за ползване на интернет услуга, такъв потребител или ще бъде лишен от ползването на интернет услуга преди края на абонаментния му период, или ще бъде таксуван с подобаваща надценка за надхвърлен интернет трафик.

Разпространение на нежелано съдържание чрез Адуер (Adware)

Адуерът (Adware) е софтуер, който се използва с рекламна цел и съответно се поддържа от реклами. След като бъде инсталиран в системата на потребителя, той започва да генерира рекламно съдържание под различна форма - изскачащи (pop-up) прозорци, рекламни банери, препратки към уеб страниците на трети лица. По този начин той генерира доход за създателите си. Използвайки уеб браузъра, адуерът може да събира и изпраща информация за активността и поведението на потребителя, като тази статистическа информация на по-късен етап може да бъде използвана за прогнозиране на предпочитанията на потребителя и подаване на рекламно съдържание, целящо покупка. Към тази информация може да бъде включен IP адресът, данни за местоположение, за операционната система и ползваният браузър, въведени от потребителя данни и др.

Най-използвани техники на разпространение на Адуер

Най-често използваните техники за разпространение на адуер могат да бъдат категоризирани като:

1. **Пакетно разпространение на софтуер** *(Бандлинг).*

Бандлингът *(bundling)* е метод на разпространение на програмни продукти във вид на пакет от програми *(bundle)*, при който заедно с основната програма в пакета за инсталация се включва страничен, платен от спонсор софтуер. Прилага се с цел рекламиране на малко известен програмен продукт, а понякога и на нежелан зловреден софтуер. Най-често се среща при предлагане на безплатни програми от типа на фриуер (freeware) и шеъруер (shareware). Повечето големи сайтове, предлагащи колекции от безплатен софтуер използват тази техника. Съществуват няколко метода за предпазване от инсталиране на нежелан софтуер при пакетния тип на разпространение:

- Изтегляне на безплатния софтуер от сайта на създателя му, а не от сайт с колекции на безплатен софтуер;

- Намиране на преносима (portable) версия на желания безплатен софтуер в проверен сайт за разпространение на преносим софтуер (примерно PortableApps.com);

- При инсталация на програмния пакет да се избира не инсталиращата по подразбиране опция, а разширените потребителски опции за инсталация *(Custom options)*, при което е възможно да се укаже инсталацията само на желания продукт.

2. **Подвеждаща официална уеб страница**.

Това е такава страница, където на един програмен продукт се приписва някаква полезна функционалност, като вместо (или съвместно) нея се предлага адуер. В някои случаи подобна полезна функционалност въобще не съществува, или се представя само имитацията и. За предпазване от тази техника на разпространение е препоръчително проучване в интернет на потребителските мнения за този продукт преди инсталацията му.

3. Фалшиви уведомления за изтегляне на ъпдейти или други софтуерни компоненти. Такива могат да бъдат инсталации или ъпдейти на браузърни разширения, известни като плъгини, изтеглянето на кодеци за преглед на видео съдържание, софтуерни компоненти и библиотеки и др.

При възникването на подобно събитие не трябва да се приема подобна инсталация, а ако такава е необходима, желателно е инсталацията да се направи от официалната уеб страница на производителя на съответния компонент или разширение.

Защити от нежелано съдържание

В този раздел ще бъдат разгледани някои разпространени защити от нежелано съдържание. Въпреки, че те са представени в отделни категории, някои от тях имат по-голяма област на действие, като за постигане на най-добър резултат може да бъде приложено комбинираното им прилагане.

1. Защита от нежелано съдържание, достигащо през уеб браузъра

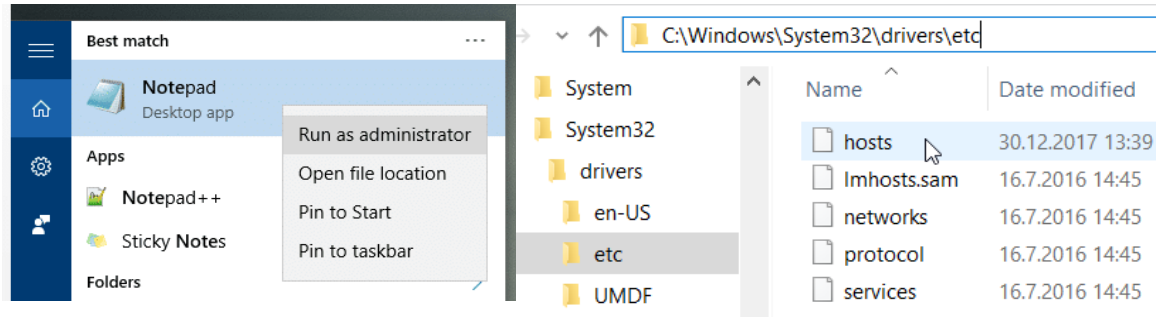
Един от най-разпространените и достъпни методи за защита от нежелано съдържание през браузъра е инсталирането на допълнителни браузърни разширения (Plug-ins) за предпазване от нежелано съдържание.

Макар, че обикновено такива представки се справят повече със защита от нежелана реклама, отколкото с предпазване от злонамерен код, широкото им използване се дължи на факта, че от потребителя не се изискват някакви специални умения и познания, за инсталацията и ползването им. Веднъж инсталирани, тези разширения се грижат автоматично за блокиране на нежеланото съдържание. Самите разширения разполагат с голям брой филтри на известни URL адреси, съдържащи нежелани реклами или съмнително съдържание. Повечето от тях доставят и опции на потребителя за добавяне на ръчна блокировка спрямо избран елемент от определена уеб страница. Някои от тях предоставят функционалност за блокиране на трасиращи "бисквитки" (cookies), малуер, социални линкове, а също така предпазват от претоварване на системата. По-добре поддържаните разширения от този тип се предоставят за най-популярните браузъри като Mozila Firefox, Google Chrome, Opera, Safari, Microsoft Edge.

Типични представители за такъв вид защита от нежелано съдържание са *uBlock Origin* и *Adblock Plus*, които се разпространяват като софтуер с отворен код (open source).

2. Защита от нежелано съдържание за всички приложения посредством локално свързване на имената на домейни.

Защитата с браузърни разширения няма как да се приложи към приложения различни от браузърните. Голяма част от тези приложения не поддържат разширения, притежават специфичен интерфейс и комутацията им със сървъри, доставящи нежелано съдържание се реализира от вграден в продукта програмен код. Поради тази причина се търсят други възможности. Едно логическото решение в този случай е прекъсване на възможността за комуникация на тези приложения с уеб базираните доставчици на нежелано съдържание. Едно такова решение е пренасочването на домейна на доставчика на нежеланото съдържание към локален IP адрес (local domain mapping). По този начин ще бъдат избягнати всякакви комуникации между приложението и доставчика на нежелано съдържание. За Windows базирани системи това става чрез отваряне на файла *hosts*, разположен в директорията *c:\WINDOWS\system32\drivers\etc\hosts* с помощта на текстов редактор като Notepad, стартиран с административни права (Фиг.1).



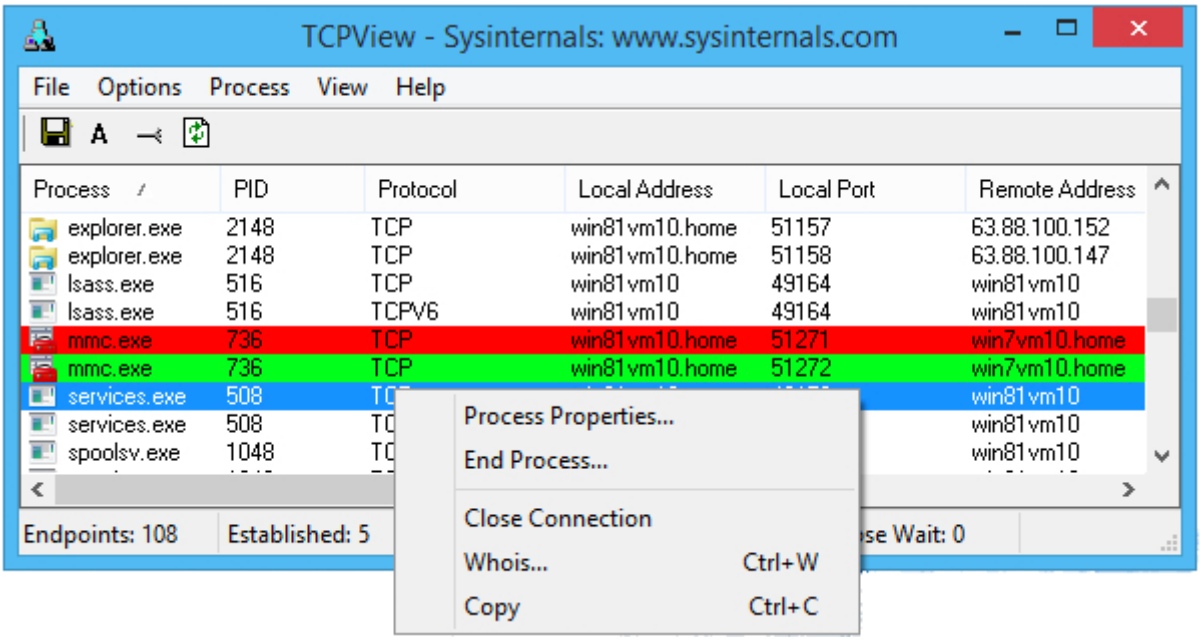
Фиг.1

Ако са известни имената на хостовете с нежелано съдържание, то обръщението на към тях може да се пренасочи към локален IP адрес на потребителската система. Присвояването на IP адрес (в случая локален) на хост става като IP адресите се поставят в лявата колона, а имената на нежеланите хостове в дясната. Понеже това е неформатиран текстов файл, достатъчно е вляво да се напиша локалния IP адрес, който ще бъде присвоен на името на хоста, да се постави пауза, а след това да се напише името на хоста на който ще се присвоява този IP адрес (Фиг.2.)

#IP адрес	**#Име на хост**
0.0.0.0	a.ads1.msn.com
0.0.0.0	a.ads2.msads.net
0.0.0.0	a.ads2.msn.com
0.0.0.0	spynet2.microsoft.com
0.0.0.0	spynetalt.microsoft.com
0.0.0.0	ads.viber.com
0.0.0.0	media.cdn.viber.com
0.0.0.0	ad.doubleclick.net

Фиг.2.

Едно от предимствата при използването на този метод, е че описаните хостове ще бъдат блокирани за цялата система, включително за всички инсталирани приложения и браузъри в системата. Съществуват огромен брой поддържани списъци, със сървъри хостващи нежелано съдържание, като съдържанието им може да се добави към списъка, съдържащ се във файла hosts. Може да се отбележи, че този метод с успех може да се използва за предпазване от малуер и адуер. За определяне на уеб адресите и хостовете, към които се обръщат приложенията може да се използват програми за проследяване на интернет трафика или свободно разпространявани инструменти като TCPView (Фиг.3) или CurrPorts.



Фиг.3

3. Защита от нежелано съдържание, доставяно чрез Адуерът (Adware)

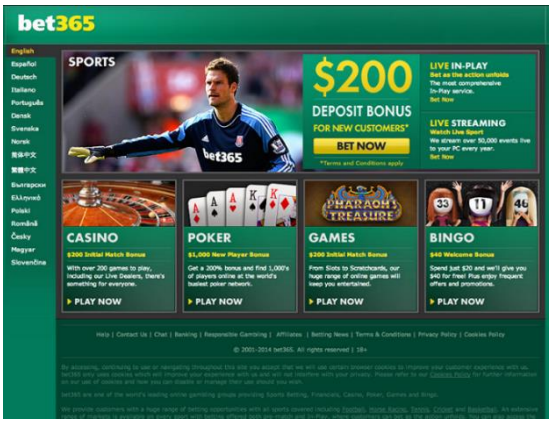
Цялостната борба с такъв софтуер в включва: предпазване, отстраняване и защита. Докато предпазните мерки, упоменати при описанието на начините на разпространение на адуера, са свързани с повишено внимание спрямо действията, предприемани от потребителя, отстраняването на адуер изисква в повечето случаи използването на специализиран софтуер.

Както бе споменато, веднъж инсталиран на потребителската система, адуерът забавя работата и, води до сривове в браузъри и приложения, и като цяло влошава работата на цялата система. Следователно е необходимо неговото отстраняване.

3.1. Отстраняване на адуер посредством специализиран софтуер

В някои случаи отстраняването на нежелан рекламиран продукт, инсталиран като част от пакетно разпространение в системата на потребителя може да бъде извършено с обичайната деинсталация на този продукт, но в болшинството случаи при инсталиране на нелегитимен адуер тази опция е неефективна. Дори и при добро познаване на основните принципи на заразяване с адуер, повечето нелегитимни адуерни продукти използват многобройни техни на заразяване и ръчното им отстраняване се явява много трудоемък процес. В повечето случаи антивирусните програми не реагират на адуер, поради различия в начина на проникване в системата, а и от функционална гледна точка е трудно да се различи адуерът от обичаен програмен продукт, използващ мрежов обмен на данни. С по-голям успех спрямо такъв вид софтуер реагират програми, предназначени за борба със шпионски (spyware) и друг зловреден софтуер (malware) известни като *anti spy* и *anti malware*. Създателите на адуер постоянно усъвършенстват използваните техники, което още повече затруднява откриването и отстраняването на нежелания софтуер. Един типичен пример в тази насока е bet365.

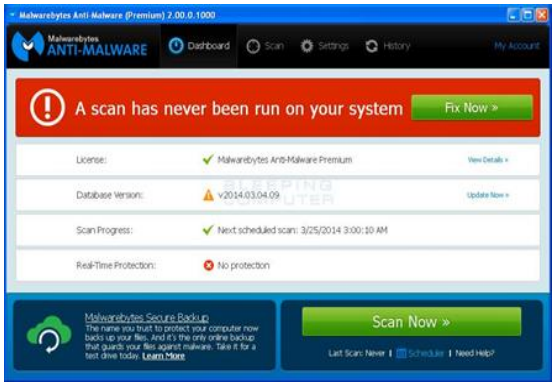
bet365.com е домейнът, до който ще бъде пренасочени потребителят, ако има инсталиран този тип adware приложение на компютъра си. Въпреки, че това не е злонамерен софтуер, той забавя компютъра, води до чест срив на браузъра, а понякога рекламата може да изложи потребителите на злонамерен софтуер, но този рекламен софтуер има за цел преди всичко да направи приходи с плащане на "клик"(pay per click), като пренасочва към bet365.com.



Инсталира се като използва описания метод за пакетно разпространение на софтуер *(Бандлинг)*.

bet365.com няма отношение с предлаганата реклама и е просто инструмент, от който хакерите се възползват, за да печелят пари, като показват реклами. Този адуер засяга всички водещи браузъри като Internet Explorer, Google Chrome и Mozilla Firefox.

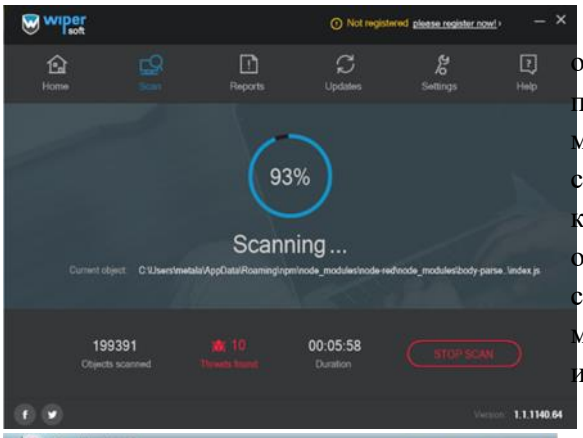
Постоянните изскачащи прозорци са основният знак, че причината за това се крие в инсталиран адуер, а не е случаен изскачащ прозорец, който се появява при посещението на определена уеб страница. Въпреки, че след първоначалната му поява, ръчното му отстраняване за конкретен браузър и операционна система беше сравнително добре описано в интернет изданията, след усъвършенстване на използваните техники от авторите му, ръчното му отстраняване се превърна освен в трудоемко и в частично решение. Това важи и за други типове адуер, поради което се налага използването на специализирани за отстраняването на адуер програми. Ще бъдат посочени някои такива продукти, предлагащи безплатен лиценз и споделени впечатленията от тях при отстраняване на адуер.



Malware bytes е продукт, създаден за борба със злонамерени програми от типа malware и adware. Предлага се като безплатна и платена версия, като в платената е включена и защита в реално време. В проведените тестове за отстраняване на адуер обаче, не бяха постигнати очакваните резултати. Това навежда на извода, че продуктът е по-ориентиран към борба с малуер, отколкото с адуер, което се подразбира от наименованието му му.

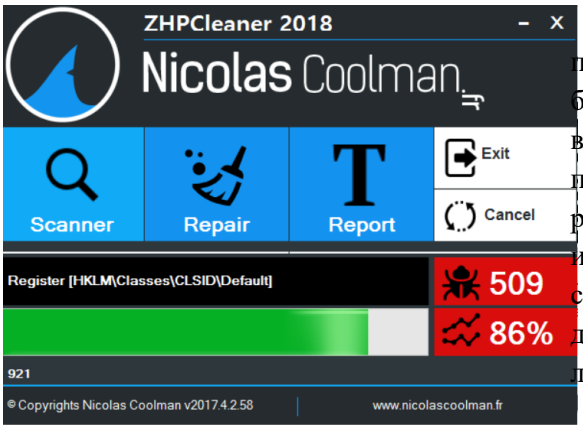
AdwCleaner е безплатен продукт, създаден за отстраняване на адуер, потенциално нежелани програми PUP/LPI (**P**otentially **U**ndesirable **P**rogram), туулбарове, и Hijack(отнемане на контрол) на началната страница на браузъра. Разпространяван от Toolsib, а по-късно, започва да излиза под логото на Malware bytes. Впечатленията при провеждане на експерименти за отстраняване на адуер са положителни.

RogueKiller е продукт, насочен към откриване и отстраняване на злонамерен софтуер от типа malware и руткит (привилегирован достъп до дадена компютърна система). Предлагат се безплатна и платени версии, които имат разширена функционалност.



WiperSoft е софтуер, за откриване и отстраняване на адуер и малуер, както и на потенциално нежелани програми. Безплатната му версия включва само възможностите на скенер за откриване на злонамерения софтуер, а комерсиалната версия позволява и тяхното отстраняване. Тестовете, проведени с този софтуер показват висока чувствителност и много добри възможности за откриване на адуер и малуер.

SpyHunter е софтуер, за откриване и отстраняване на адуер и малуер, както и на потенциално нежелани програми. Както и при Wipersoft, безплатната версия включва само възможностите за откриване на злонамерен софтуер, а комерсиалната версия позволява и тяхното отстраняване. При провеждане на тестове с този софтуер, бяха получени много добри резултати при откриването на адуер и малуер.



ZHPCleaner е безплатен софтуер, предназначен да се бори с похитителите на браузъри (Hijackers). Основната цел е възстановяването на прокси настройките, премахне препратките на браузърите. Премахва рекламните програми, които показват изскачащи прозорци, потенциално нежелан софтуер, някои ленти с инструменти, нежелано добавени към браузъра, някои ненужни легитимни програми.

3.2. Защита от нежелано съдържание, доставяно чрез адуер и сайтове, доставчици на адуер посредством DNS блокиране и филтриране

Разгледаните досега методи включваха използването на браузърни разширения, филтри за хостове-доставчици на нежелано съдържание и пренасочване на техните домейни към локален адрес на компютърната система. Въпреки ефективността на последните разгледани методи, съществуват трудности от прилагането им от редовия потребител, свързани с корекцията на хост файла, добавянето на списъци от пренасочващи филтри в него и актуалната им поддръжка или изследване на интернет връзките, осъществявани от специфично приложение. Подобни техники за филтриране и пренасочване обаче се използват от предоставяни интернет услуги, използващи DNS (**D**omain **N**ame **S**ystem) блокиране. Основното предназначение на системата за имена на домейни е улесняването на мрежовата комуникация на потребителя. Известно е, че компютрите в мрежата комуникират посредством IP адреси примерно: 176.103.130.130 за интернет протокол версия 4 (IPv4) или 2a00:5a60::ad1:0ff за интернет протокол версия 6 (IPv6). Този вид представяне на адресите за комуникация не е подходящ за запомняне от хора, поради което възниква необходимост от система, каквато се явява системата за имена на домейни. Тя може да бъде разгледана като регистър (състоящ се от множество сървъри), в който на определен IP адрес се назначава определено име (регистрация на домейн). По този начин потребителят първоначално се обръща към лесно за запомняне име,

след което заявката се изпраща към системата с имена на домейни, която връща реалния IP адрес на компютъра, към който е отправена потребителската заявка. Операционните системи, както и рутерите позволяват настройка на предпочитан и алтернативен DNS сървър. Следователно за филтриране на нежеланото съдържание е достатъчно, указването на адрес на DNS сървър, предназначен за блокиране на доставчици на нежелано съдържание. Примери за такива сървъри са OpenDNS, AdGuard DNS, Alternate DNS, Comodo Secure DNS и др. При прилагане на такава защита на ниво рутер, от нежелано съдържание ще бъдат предпазени всички устройства, ползващи мрежовата комуникация през рутера. Недостатъците при този тип защита са свързани най-вече със забавяне на времето на реакция на DNS сървъра при използване на отдалечен или натоварен такъв, което забавя работата в интернет.

Сравнителни характеристики на описаните методи за защита от нежелано съдържание			
Вид защита:	**Област на действие**	**Предимства:**	**Недостатъци:**
Браузърни разширения	Конкретен браузър (на който е инсталирано разширението).	Лесна за инсталация, не изисква поддръжка от страна на потребителя.	Защитата се отнася само до браузъра на който е инсталирано разширението.
Локално свързване на хост имената	Всички апликации и браузъри, инсталирани на потребителската система използващи мрежова комуникация.	Възможност за пълен контрол над блокирането на съдържанието. Не е свързана с намаляване на бързодействието.	Необходимо е назначаването на права за модификация на хост файла. Изисква се ръчно въвеждане на списъци с хостове за блокиране.
Външна DNS услуга	- Цялата потребителска система при използване на ниво "операционна система"; - Всички потребителски системи, ползващи интернет трафик през рутера при използване на ниво "рутер".	Не се изисква поддръжка от страна на потребителя; Разширена област на действие на защитата при използването и в рутера.	Възможни забавяния в интернет заявките при натоварен или неподходящо подбран външен DNS сървър.