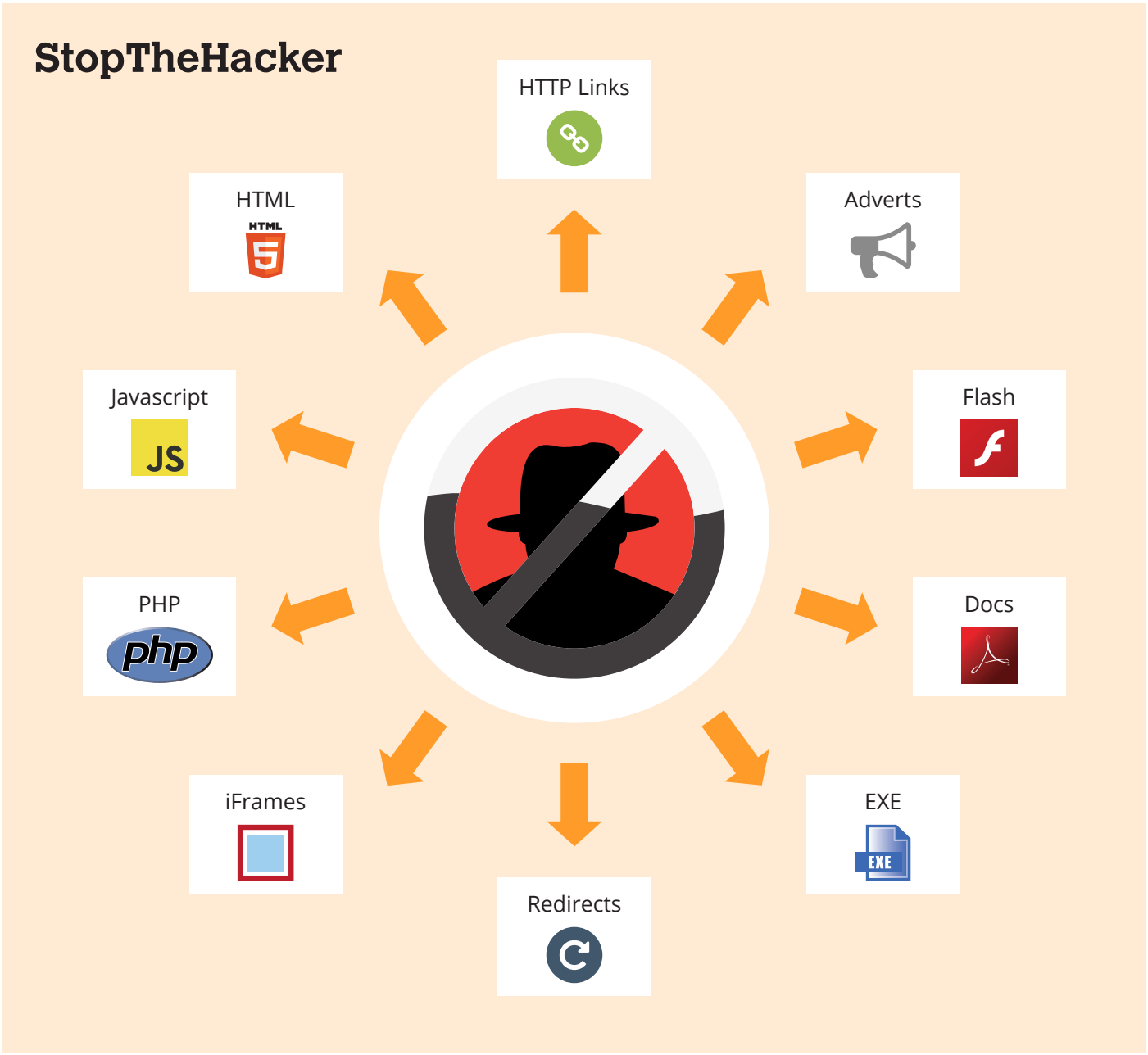
StopTheHacker

Data Sheet

Secure your website and your reputation

> "Just like all PCs need anti-virus, all websites need malware protection."

Google currently displays 3 million warnings of unsafe websites to 400 million users every day[1] and it is estimated that approximately 4% of all hosted websites are infected with malware at any given time. Website hacking and malware are two of the most common methods used by external agents to breach a website. Research conducted by Verizon[2] found that 92% of all breaches came from external agents using multiple methods to achieve their goals, with 89% utilizing some form of hacking and 79% incorporating malware. StopTheHacker Pro provides your website with an advanced feature-set to provide comprehensive protection for your website and your website visitors from malware.



StopTheHacker is not anti-virus software

Anti-virus (AV) software is slow to identify new threats and this delay allows malicious content to stay undetected for longer. AV engines only focus on analysing traditional malware for the most part like EXE, MSI, and SCR files. The way to analyse these files is different than analysing malware written in dynamic Web 2.0 languages like PHP, ruby, HTML, JavaScript etc.

StopTheHacker profiles web-malware code to understand features of a piece of code, such as how many arrays and variables are used, how they are used, who is using them, how many times over, etc. All give tell-tale signs of whether this is legitimate usage or malware-like behavior.

- AV engines cannot detect malware injected inside .htaccess files, StopTheHacker can
- AV engines cannot detect malware injected via ads, StopTheHacker can
- AV engines cannot detect malware injected as CSS, or inside CSS files, StopTheHacker can

Key Benefits

Cloud-based software

StopTheHacker is a fully hosted software solution to provide your website with advanced website security and monitoring tools. There are no changes required on your website or any software for you to install.

Protect your business and your revenue system

Getting your website banned from the search engines or being identified as the source of malware on a customer's computer would be detrimental to any business. StopTheHacker is your proactive business tool to make sure this does not happen.

In-depth analysis of your website

AV engines use databases of malware sites to determine whether a link that is leading away from a web page is good or bad. StopTheHacker goes beyond databases and checks the landing page for malware code.

StopTheHacker FAQs

What is malware?

Malware is software designed to disrupt computer operation, gather sensitive information, or gain unauthorized access to computer systems. While it is sometimes software, it can also appear in the form of script or code. Malware is a general term used to describe any kind of software or code specifically designed to exploit a computer, or the data it contains, without consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software. Malware includes computer viruses, worms, trojan horses, spyware, adware, most rootkits, and other malicious programs[3].

I use one of the world's most popular CMS for my website, surely I am safe?

Hackers are experts in finding exploits on websites and using them to gain access. For example, if your website uses third-party plug-ins or scripts this is a common approach hackers will take to gain access.

What are blacklists?

As a public service, companies such as Google analyse websites and determine if the website is distributing malware or has been reported as taking part in a phishing attempt. If this is the case, the website is removed from their search results and most web browsers will alert visitors to the threat your website poses.

What happens if malware is detected?

You will automatically be alerted to any malware found during a scan. Additionally, if Malware is detected on a file, you can restore your website back to a previously stored clean version quickly and easily.

Sources

1. http://www.networkworld.com/news/2011/081811-google-highlights-trouble-in-detecting-249850.html
2. http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf
3. http://en.wikipedia.org/wiki/Malware