





September 28, 2011

Protecting The Reputation Of Your Online Business

Websites are the new battleground between malicious hackers, security professional and online business owners. The game has changed, malicious hackers are targeting websites in order to compromise them, steal precious business information and employ legitimate benign websites to do the dirty work for them. Malicious hackers are no longer focusing on defacing websites, their motivation has morphed. Websites are hacked to be used as distributors of malware, to infect millions of visitors unknowingly with viruses and malware. These kind of attacks destroy the reputation of more than 6,600 websites every single day. It is imperative to sit up and take notice, and employ mechanism which will protect your website against these kind of devastating attacks.

What is the problem:

Websites are under attack, as hackers find new ways to make money off the web. The web-security war is where the anti-virus war was ten years ago. At the heart of the matter lies *code injection*, a new cyber-crime proliferation mechanism that introduces malicious code or hyperlinks in compromised websites. The hackers hurt the visitors of the website, by infecting their computers, or performing identity theft. Although the hackers do not harm the website directly, the website can be blacklisted by search engines ruining its online reputation.

What Visitors See When Your Website Gets Hacked	Google Discourages Visitors From Clicking Through To Your Website
 <p>Warning: Visiting this site may harm your computer</p> <p>The website you are visiting appears to contain malware. Malware is malicious software that may harm your computer or otherwise operate without your consent. Your computer can be infected just by browsing to a site with malware, without any further action on your part.</p> <p>For detailed information about problems found on this site, or a portion of this site, visit the Google Safe Browsing diagnostic page for l0f0s0.c0.b0.</p> <p>Ignore Warning Go Back</p>	 <p>Google <input type="text" value="example.com"/> <input type="button" value="Search"/> Advanced Search Preferences</p> <p>Web</p> <p>Example Web Page This site may harm your computer.</p> <p>You have reached this web page by typing "example.com", "example.net", or "example.org" into your web browser. These domain names are reserved for use in ... www.example.com/ - 1k - Cached - Similar pages</p>

Consider the fact that more than 6,600 benign websites are getting hacked every single day. These legitimate websites are turned into distributors of malware by malicious hackers. Once a website is identified as a distributor of malware, search engines such as Google, Yahoo, Bing and other will “blacklist” that website. As a result all modern browsers, which query these blacklists in order to protect Internet users from inadvertently landing up on malware infested sites, will block access to your compromised website. This deprives your business of potential customers and visitors and tarnishes your online reputation significantly. The screenshot below shows what your potential customers will see in Firefox, Safari, Internet Explorer, Opera and other browsers, if your website gets hacked. We also show how Google discourages Internet surfers from visiting hacked websites.

Is my website at risk: More than 95% of websites in the Internet have at least one major security hole which can be exploited by malicious hackers to break in and cause havoc. Thousands of websites get hacked every day. Most websites are hosted by professional web-hosting companies who may not have the necessary security

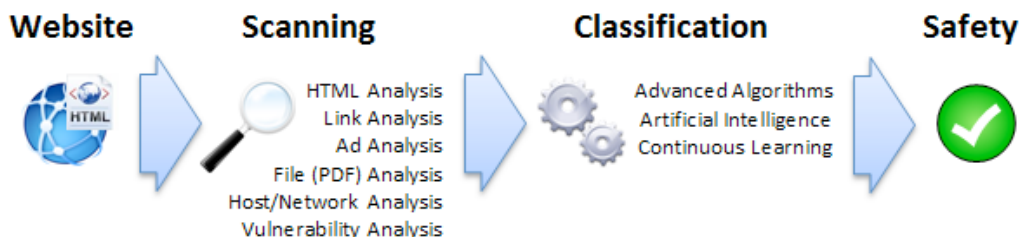
expertise to safeguard your business from attacks like these. Furthermore, attack patterns are constantly changing. This is an evolving battleground. Only websites that employ constant vigilance can beat back the hackers.

Every website is a target, businesses, government and military websites, and web hosting companies (“*Webhost hack wipes out data for 100K sites*”, VAServ Ltd hosting, 06/2009). The incidents are increasing at a rate that hints at a pandemic (“*Malware: Another pandemic of which you need to be aware*”, EDNews, 05/2009).

Our services: Our services are offered on Software as a Service (SaaS) basis, and they are run outside the firewall. There is no software to install, and no need to change anything: just one more powerful security tool in one’s security arsenal. Our services are complementary to, but different from anti-spam, anti-virus, or firewalls.

- 1. Notification:** E-Reputation Monitoring notifies customers if search engines blacklist their site(s).
 - 2. Detection:** Health Monitoring (HM) periodically checks websites to detect injected malware to prevent blacklisting, and pinpoint the location of malicious code.
 - 3. Prevention:** Vulnerability to Penetration Assessment (VPA) is an in-depth automated penetration testing of the security of the website and provides actionable tips for hardening a site against intrusions.
 - 4. Recovery:** Recovery is a consulting service to help remove a website from search engine blacklists.
 - 5. Trustmarks:** Customers may display our Security Trustmarks, which are known to increase visitor’s confidence (reportedly an 11% increase in sales).
- Pricing: \$3 to \$500 a month on average depending on level of service and no. of pages.

The Benefit: Our services can reduce the operational cost of a company by: **(a) avoiding intrusions** by hackers, **(b) protecting the online reputation of a company** and keeping it off the blacklists of Search Engines, such as Google and Yahoo, and **(c) reducing a company’s IT cost** by reducing the workload and the number of IT professionals needed.



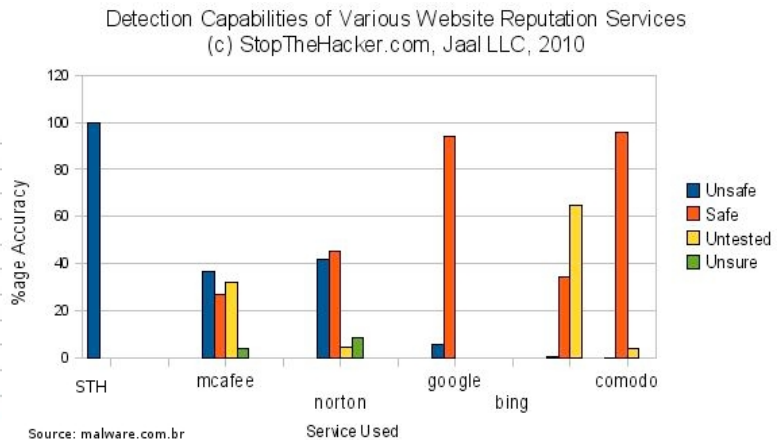
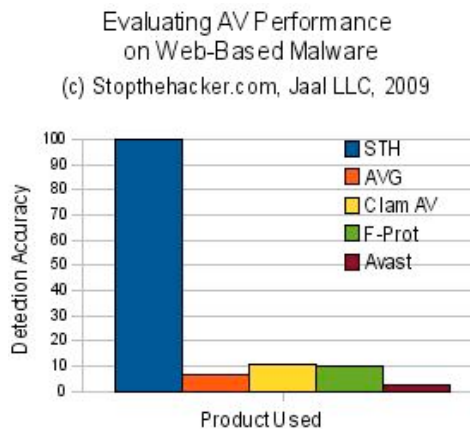
Our Advantage: We are focused on web security, and we are in the forefront of technology. We have developed a number of proprietary, patent-pending algorithms and automatically synthesize and integrate the information from many different tools using Machine Learning and AI techniques with self-adapting capabilities. The novelty of our technology has been recognized by award no. 0839491 from the National Science Foundation.

How can my website be compromised: Websites can be compromised in many ways. Most modern websites use pieces of software (e.g. CMS like Wordpress, frameworks like Joomla, Django etc.) that is re-used by website designers and programmers. These re-usable pieces of third party computer software can contain vulnerabilities and can allow malicious hackers to break into your website. Furthermore, website hosting companies may not be able to provide timely updates and upgrades for the software powering your website which leads to open security holes. Additionally, custom computer code developed by website designers often contain security vulnerabilities because most website developers are not sufficiently trained to write secure computer code.

What happens if my site gets compromised: If your site gets compromised and is misused to distribute malware to innocent visitors, the infected website is put on a “blacklist” by various search engines such as Google, Yahoo, Bing and others. Most modern browsers seek advice from these blacklists and attempt to protect Internet surfers from landing up on infected websites. When users try to visit your website, they will be blocked from doing so by their browser. This will lead to loss of revenue and visibility in the Internet. Moreover there will be an irreparable loss to the reputation of your website and business. Additionally, the recovery process to clean up a website, after an extensive attack, not detected in time, will prove to be very expensive. Furthermore, the amount of money you have invested in Search Engine Optimization (SEO), in order to appear favorably in

search engine results, will be put to waste. In short the results of getting blacklisted are extremely grave and unfavorable.

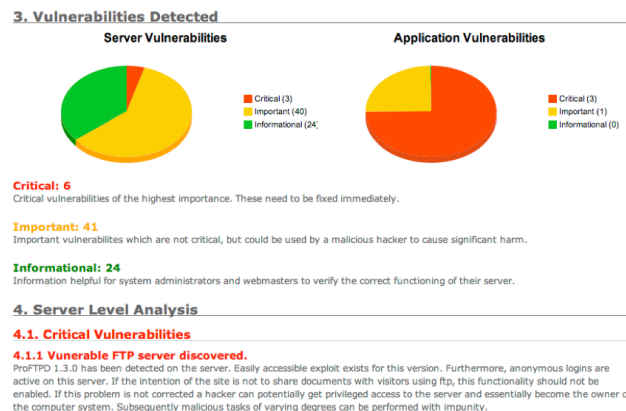
Will my Antivirus not protect me: Unfortunately, detecting web-based malware is very different than detecting malware which traditionally infects a personal computer. See below how Anti-Virus engines are poor at detecting web-malware on webpages. Even services which claim to provide website reputation services are not accurate, see below.



What can I do to stop this from happening to my website: There are many best practice mechanisms which you can employ. A lot of useful information is listed on our FAQ pages: <http://www.stopthehacker.com/faq/>.

To protect a website from malicious hackers, it is imperative to monitor the reputation of the website continuously, detect signs of any malware infection, assess the security level of the website on an ongoing basis. It is important to use a service which evolves constantly with the morphing techniques which hackers use to infect websites. To stay a step ahead of the hackers, is not easy for traditional Anti-Virus companies, which use signature based mechanisms to detect malware. Services, such as Stopthehacker, which use machine learning and Artificial Intelligence based malware detection are miles ahead of other services.

How can Stopthehacker.com help: Stopthehacker's advanced services can protect the reputation of your online business and website. Stopthehacker's advanced technology, depicted below, constantly evolves to stay a step ahead of the malicious hackers. Stopthehacker's online dashboard, see below, lets you take complete control of your website, allowing you to pick and choose the right security service for your needs. Protect your website today, and insure your business's online reputation.



For any clarifications please contact: Anirban Banerjee, a.banerjee@stopthehacker.com