HackAlert™ FAQ

Table of Contents

1. What is HackAlert™?

Armorize HackAlert™ is a cloud-based Web malware monitoring and detection service that immediately notifies subscribers if their website is targeting end-user Personal Computers (PCs) with Drive-by Downloads.

Delivered as a hosted Software Service (SaaS), HackAlert™ protects businesses and customers from the impacts of Malware Injection.

2. What is a Cloud-based Service?

A cloud-based service leverages the principles of cloud computing to deliver computer-based business applications.

In cloud computing, application details are abstracted from the users who no longer need knowledge, expertise or control over the underlying infrastructure. Instead, service providers utilize the Internet (i.e. the "Cloud") to provide scalable and virtualized resources as a web-based service.

For HackAlert™, the only client requirement is a web browser, Internet access and the necessary credentials to access the service. The application is presented through a web interface while business logic, software and data are handled on the Armorize server infrastructure.

3. What is meant by Software as a Service (SaaS)?

Software as a service (SaaS) is a software deployment model based on cloud computing. With SaaS, a provider licenses an application to customers as an on-demand service. The software itself is hosted on the provider's own infrastructure or at commercial accredited datacenters that offer virtualized server access. As per the definition of cloud computing, the SaaS is accessed through a web interface with all business logic, processing and storage handled by the provider.

4. How does HackAlert™ address injection and malware Drive-by Downloads?

HackAlert™ monitors websites around-the-clock for malware injection. The service immediately notifies subscribers if their website is initiating malware drive-by downloads that target end-user computers. The overall HackAlert™ scanning and analysis process is outlined in Figure 1.

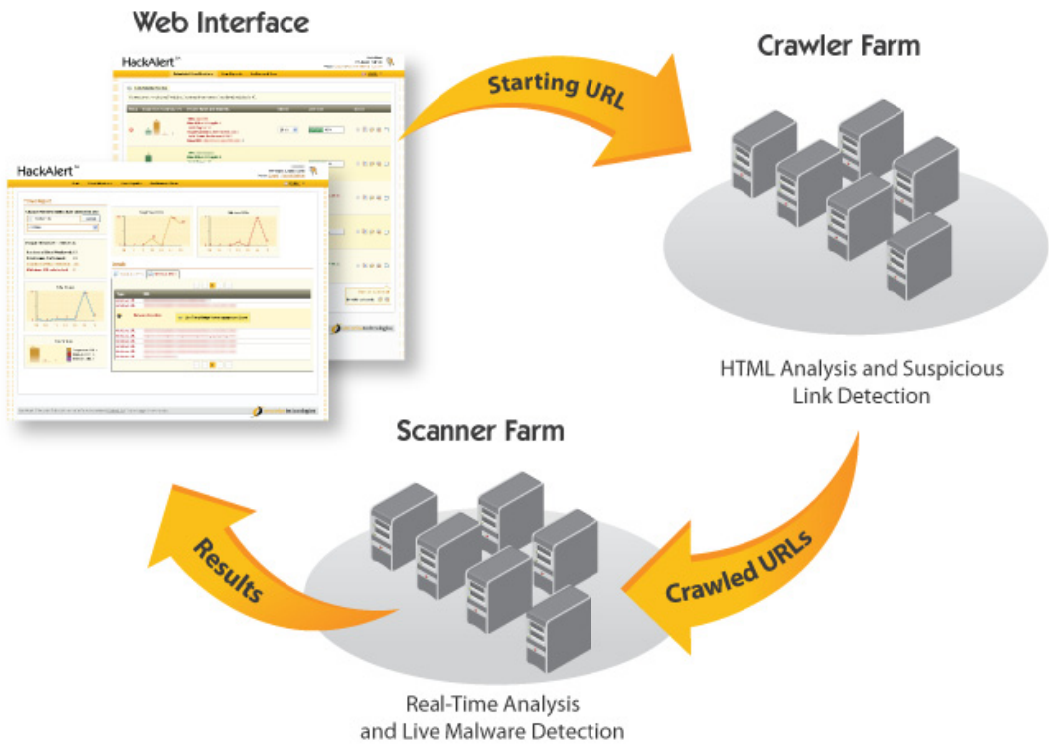

Figure 1: HackAlert™ Scanning and Analysis Process

The behavior-based scanning engine not only identifies active malware downloads but also compares its findings to Google's malicious site lists to facilitate verification of the site's blacklist status.

If the monitored site is actively distributing malware, HackAlert™ will provide information such as malware behavior, the injected code snippet, vulnerability exploit details and remediation guidance. If the site has also been flagged by Google as malicious, HackAlert™ will report this along with steps to quickly remove this flag.

If the website is not actively propagating malware but is still flagged by Google, HackAlert™ will also report this and will provide reasons for the discrepancy along with the steps to quickly update this status.

HackAlert™ also offers mitigation through its optional recovery module. Installed as a web server plug-in, this module removes malware from outbound HTTP responses to prevent drive-by downloads in real-time.

Available a true cloud-based service (SaaS) and as an enterprise monitoring system API, HackAlert™ represents a

critical component of the Incident Response process by ensuring that administrators can react immediately to malware injection to protect corporate and client resources.

5. What is meant by the term "behavior-based scanning engine"?

HackAlert™ does not rely on signature matching to detect malware drive-by downloads. The service connects to the subscriber website using a standard HTTP connection. HTTP responses are downloaded to an isolated "sandbox" environment hosted at the Armorize datacenter where they are automatically analyzed for behavioral characteristics that indicate malware injection. If there is an active drive-by download, the actual downloaded file's behavior is analyzed and reported back to the subscriber.

6. What are the advantages of behavior-based analysis

Behavior-based analysis provides the following benefits:

- **Increased accuracy:**

Signature-based malware solutions such as those offered by commercial antivirus vendors have the following disadvantages:

- Once new malware is released, antivirus vendors must analyze it and create a signature for it. This means that commercial antivirus solutions offer no immediate protection for new (zero-day) malware. This often remains the case for many days after release.
- Web application hackers have learned to pack or obfuscate malware in a variety of formats that make signature-based detection all but impossible.

On the other hand, as a true behavioral analysis solution, HackAlert™ is not dependent on vendor-defined signatures but instead analyzes the actual behavior of an application to determine whether or not it contains malware.

Malware behavioral analysis offers far greater accuracy than signature-based technology along with immediate capability to detect zero-day malware.

Detailed behavioral information

HackAlert™ connects to the monitored website over a standard HTTP connection and captures all responses in deliberately unsecured "Honey Clients" located at Armorize data centers worldwide. All website responses are analyzed for the presence of both active malware content and suspicious links (to external sites not currently distributing malware). This distinction greatly reduces the amount of false positives.

HackAlert™ reporting delivers the following details:

- URL that has been injected
- Injected code snippet details
- Browser vulnerability that the drive-by download exploits
- Malware behavior details such as:
  - Whether it is active malware or a simply a suspicious link[1]
  - Malware download file name
  - Source URL, i.e., where the compromised site retrieves the malware from
  - Download destination on target computer

Detailed remediation Guidance

As HackAlert™ actually captures the website's HTTP responses, it is able to specifically pinpoint injected code snippets to aid mitigation. Reporting also provides details of the actual browser (or browser extension) vulnerability that the malware attempts to exploit.

HackAlert™ also compares the true website malware injection status with that being reported by Google's safe Browsing index reported at http://www.stopbadware.org.

7. How does Malware Injection Monitoring differ from Web Application Scanning?

Malware Injection Monitoring

Malware injection monitoring connects to the website over a standard HTTPport and analyzes all responses for the presence of malware. It does not attempt to exploit application vulnerabilities and does not impact the running application through intrusive scanning.

Web Application Scanning

Web Application Scanning - often referred to Penetration Testing - is also known as "Black Box" testing as it is conducted from the perspective of the hacker probing the running application. Web application scanning tools are typically client-based software applications that scan live Web applications, locating entry points and executing multiple attack variants based on the vendor-supplied signature database. These scans may be intrusive when the application is vulnerable to an attack signature that causes it to crash.

[1] *A suspicious link is defined is a link to a 3rd party website that meets certain conditions up to but not including active malware downloading. It is considered suspicious as opposed to malicious because although it was likely injected for malicious purposes, at the time of the scan it is not downloading malware. By making this distinction, HackAlert™ provides a more accurate picture of the hacker's behavior and helps to greatly reduce false positives.*

8. How does malware injection monitoring differ from antivirus software?

Malware Injection Monitoring

HackAlert™ is a cloud-based software service that monitors subscriber websites to detect and mitigate malware injection and Drive-by Downloads from websites. Honey-clients located at the Armorize datacenter browse subscriber websites and analyze the HTTP responses potentially malicious links and active malware downloads. HackAlert™ does not rely on signatures and is thus best suited for to detection of zero-day attacks.

Antivirus Software

Antivirus software is installed on the host being protected and is designed to detect and isolate malware attacking that host. In order for malware to be detected, the malware signature must be on the host. This is typically downloaded in the form of a vendor-supplied update files. The latency between malware releases and the corresponding signature along with improvements in obfuscation and packing techniques make host-based antivirus an increasingly less effective anti-malware solution.

9. How does HackAlert™ differ from signature-based malware injection monitoring tools?

Unlike signature based malware detection tools, HackAlert™ does not rely on the Google Safe Browsing Index for reporting and analysis. Instead, with its 24x7 scanning, it ensures that website owners can detect and remediate Malware injection **before** the next Google index cycle. In this manner HackAlert™ prevents Google blacklisting.

HackAlert™ also verifies websites' Google blacklisting status. For sites that have already been flagged and listed on http://www.stopbadware.org, HackAlert's behavioral analysis engine can actually test the website's true status. It will verify whether or not malware is present and will provide details on how to remove the malware and on how to remove the website from the Google blacklist.

10. How does HackAlert™ help website users?

HackAlert™ helps protect website end-users by notifying the website owner immediately if their site is injected with malware or is pushing drive-by downloads computers browsing it. This protects users browsing the website from malware injection and ensures that customers' personal information is protected.

HackAlert™ also supports automated remediation through its optional web server module. This ensures that malware drive-by downloads can be prevented in real-time.

11. How does HackAlert™ help businesses?

As a critical component of the malware injection incident response process, HackAlert™ helps safeguard website users from malware and thus:

- Ensures the website is not flagged by as a source of malware
- Prevents search engine flagging and blacklisting
- Enables compliance with standards such as PCI
- Preserves overall business reputation

12. How are HackAlert™ scans managed through the web console?

HackAlert™ is accessed through an Internet-based web console that allows subscribers to enable on-demand or automated web site scans. The Web 2.0 interface supports configuring scan schedules, report distribution options, and scanner crawling depth.

Figure 2: HackAlert Website Monitoring Configuration

13. What is website crawling?

HackAlert™ is designed to monitor entire websites as opposed to just single URLs. When configuring a new website monitoring project, the initial URL is specified. HackAlert™ will scan that page as well as every page that is linked to on that page. This will continue until the maximum depth or number of pages to be scanned is reached.

Crawling depth is defined as the number of consecutive links from the home page to each page within the web application. For example if it takes 3 clicks to get to a specific page within the application then it can be said that the page has a depth of 3.

14.How is the HackAlert™ API utilized?

The HackAlert Application Programming Interface (API) allows developers to integrate the HackAlert™ core engine with their applications. Sending JSON requests via HTTP to the API URL, they can control HackAlert™ functions such as crawling, scanning and analysis from within their own enterprise security management systems, threat feeds or custom malware reporting tools.

15.What information is contained in HackAlert™ alerting and reporting?

HackAlert™ reporting delivers the following details via email and SMS as well as within the Web console:

- URL that has been injected

- Injected code snippet details
- Browser vulnerability that the drive-by download exploits
- Malware behavior details such as:
  - Whether it is active malware or a simply a suspicious link[2]
  - Malware download file name
  - Source URL, i.e., where the compromised site retrieves the malware from
  - Download destination on target computer[3]
- Detailed remediation Guidance
- Comparison with malware injection status as reported by Google along with remediation steps if required

16.How can I use the HackAlert™ report to recover from injection?

HackAlert™ ensures that website owners can identify not only the URL on their website that has been injected but also the source URL from where the browser retrieves that active malware. HackAlert™ provides the actual injected code snippets to aid in immediate removal and to support identifying the name of the actual downloaded file.

17.Does HackAlert™ support automated mitigation?

HackAlert™ automatically integrates with the web server to provide instant mitigation. Upon detecting malware injection, HackAlert™ communicates with the optional web server module which dynamically removes injected malicious elements from outbound HTTP responses.

The web server module prevents drive-by downloads in real-time and supports all common web server platforms including FreeBSD, OpenBSD, Linux, and Microsoft Windows[4].

18.How does HackAlert™ address false positives?

HackAlert™ relies on analyzing the actual web application behavior as opposed to simply relying on malicious code and exploit signatures or feeds from Google's Safe Browsing API.

By analyzing the actual HTTP responses, HackAlert™ identifies active malware downloads and suspicious links. HackAlert™ will always identify files in the HTTP download stream. It is highly unusual for legitimate web applications to silently download files to computers browsing it so it can be assumed that these files are typically malicious and that there will be no false positives.

[2, 3, 4] – These are optional components that are not necessarily available on all HackAlert™ deployment

It is common for links in injected iframes or javascript to be inactive. Once a hacker has compromised a web application in this manner, they may add, remove and change the active malware download at will. If during a HackAlert™ scan, it is found that there is an injected link with no active malware download, HackAlert™ will flag it as suspicious as opposed to malicious. This is to ensure that the website owner is aware that this may very soon become malicious. Note that not all HackAlert™ distributions support suspicious link detection.

19. How does HackAlert™ address false negatives?

For active malware, HackAlert™ will always detect the malware in the download stream and will therefore have zero false negatives.

For suspicious links HackAlert™ will always test iframes, javascript and obfuscated code to determine whether there it leads to malware. Even if there is no malware downloaded, the code will be flagged as suspicious. If the suspicious link detection capability is not availabile, injected links that do not result in active malware downloads will not be reported.

20. How do the HackAlert™ honey clients represent standard browser configuration

The HackAlert™ honey clients at the Armorize datacenter are designed to represent a "normal" Internet user's computer. The operating system and Internet configuration represents the lowest common denominator in terms of security. The bulk of new malware that appears is capable of exploiting this configuration to some extent. While theoretically, specific attacks could be crafted to target very specific configurations but in general they will always compromise the HackAlert™ build. This ensures that HackAlert™ has the broadest coverage possible.

21. Will HackAlert™ impact a Web application's performance?

HackAlert™ connects to the monitored website over standard HTTP connections at intervals defined by the subscriber. The scans are non-intrusive and all analysis is conducted by the service on computing systems hosted at the Armorize datacenters. Therefore, HackAlert™ has no impact on web application performance.

22. Does HackAlert™ require any software installation?

HackAlert™ requires no software installation on either the websites being monitored or on end-user PCs. The service is hosted at Armorize Technologies' global datacenters and is accessible to subscribers via a Web 2.0 interface.

23. Is HackAlert™ dependent on the Web application development language?

HackAlert™ can monitor any website for malware injection regardless of the programming language used to create it. The HackAlert™ service simply makes standard HTTP connections to the website being scanned.

24. Does HackAlert™ require access to source code, binaries or debug information?

HackAlert™ requires no access to application source code, binaries or debug information. The HackAlert™ service simply makes standard HTTP connections to the website being scanned.

25. Are HackAlert™ trial accounts available?

HackAlert™ is available as a free online trial. The only requirement is a standard web browser. To register for a HackAlert™ trial please visit http://hackalert.armorize.com or email trial@armorize.com .