

Cisco shines light on dark corners of the Web

October 9 2009, by Glenn Chapman



Cisco IronPort Web Usage Controls promise to identify as much as 90 percent of "egregious" content that has escaped detection by business IT managers and security applications because of its stealthy nature on the Internet.

Cisco launched software that shines light on potentially troublesome websites hidden in what the US computer security firm dubbed the "Dark Web."

Cisco IronPort Web Usage Controls promise to identify as much as 90 percent of "egregious" content that has escaped detection by business IT managers and security applications because of its stealthy nature on the Internet.

"The Dark Web is about corporate users' inability to see how workers are using the Web," [Cisco](#) product line manager Kevin Kennedy told AFP on Thursday.

"It is that dark, dynamic and churning part of the Web that has created the problem for business."

Computer users are growing increasingly savvy about sidestepping Internet filters, using proxy servers and other techniques to mask which websites they visit while at work, according to Cisco.

For example, if workers log into Facebook.com from an office computer someone in the IT department can typically tell how much time they fritter away at the popular [social-networking website](#).

However, if the employee connects to Facebook through any of thousands of proxy websites set up daily all an IT department monitor will see is a nondescript [Internet address](#) as the online destination, Kennedy said.

Blocking porn websites on work computers typically involves using filter software based on lists of known online adult-content locales.

Internet porn purveyors have taken to constantly changing URLs, Internet addresses, in a practice referred to as "churning," according to Cisco.

"It's happening and businesses don't necessarily see it," Kennedy said of workers circumventing company constraints on online access to websites for gambling, porn, hate speech and other material that can cause legal woes.

"Most people are pretty well behaved at work, but some are not," Kennedy said.

"Using an anonymous proxy is sophisticated to us, but the kids that have graduated from colleges in the past five years are very aware of using

software to get to proxies."

The Dark Web has been formed largely as a result of tidal wave of Web pages triggered by Web 2.0 trends in user-generated content such as blogging and social networking, according to Cisco.

Only 20 percent of the more than 45 billion websites in the world are reportedly categorized effectively enough to be used by filtering programs, leaving 80 percent of the Web in the dark.

"Legacy approaches only give a small view now that there is this explosion of user-generated content online," Kennedy said. "We as an industry have to do better at how we solve this problem."

Tests of Ironport Web Usage Controls reportedly identified 50 percent more off-limits websites than did previous-generation filtering software relying on website address lists.

Ironport combines list-based filtering of known websites with a "dynamic engine" that reads [Web](#) pages to decide in real time whether content on them is something businesses don't want workers to access on company time.

Ironport software is also trained to recognize proxy servers, according to Kennedy.

"We are doing pretty well; there is room for improvement," Kennedy said. "You have to balance between catch rate and false-positive rate."

False positives are times when filtering software blocks access to websites that don't deserve to be off-limits by company standards.

(c) 2009 AFP

Citation: Cisco shines light on dark corners of the Web (2009, October 9) retrieved 4 April 2024 from <https://phys.org/news/2009-10-cisco-dark-corners-web.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.