

# Memorandum

To: Security Service Clients  
From: Tom Dedman *Tom Dedman*  
Subject: Unblocked FTP Attempts for Week of April 5  
Date: April 12<sup>th</sup>, 2010

---

This past week we again experienced 2 events where connections attempts were made to our Web site hosting server.

In the normal course of business, if an attack was not blocked by our Intrusion Prevention System (IPS), we will contact the client impacted as a part of our course of remediation. Since similar events were reported to you last week I wanted to continue with the events occurring during the week of April 5<sup>th</sup>.

The attacks identified in this past week are what the industry terms a 'brute force' attack against the CUsource FTP service running on the server that hosts the web pages for many of your organizations. Brute force attacks typically consist of a machine that is programmed to continually attempt to login to the account(s) using common passwords. Because FTP connections are normally used to upload information to these sites by their owners, FTP connections are not blocked by the IPS.

On Thursday the 8<sup>th</sup> 1,160 brute force attempts were recorded by SecureWorks with 1,150 to the WS-FTP Service and 10 to the old uniprosystems.net site. The source IP address indicates that these attempts were all coming from Saudi Arabia.

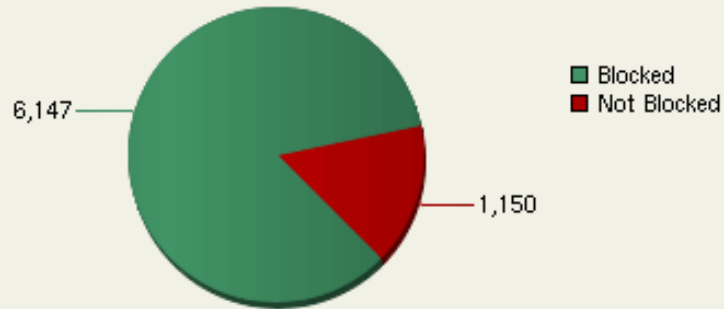
In response to these events, and the events reported to you last week, CUsource staff has elected to block all access to ftp services in our operations from any networks that are located outside of the North American continent at our perimeter. In addition we completed a thorough review of the FTP connection logs on the web server to confirm that all of the 1,160 connection attempts failed to allow access to the targeted sites.

A copy of this week's summary report is attached for your review. Please let me know if you have any questions or concerns. You can reach me by email at [tomd@cusource.com](mailto:tomd@cusource.com) or by phone at (800) 430-0215.

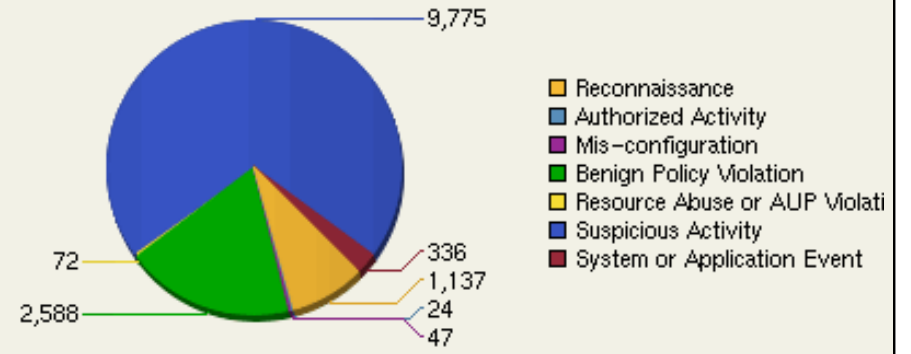
**Title** Executive Summary: iSensor F-06667, iSensor\_F-05300 Group  
**Subtitle** Executive Summary for Mon Apr 05 2010 - Mon Apr 12 2010  
**Inspector** CUSource, LLC.

[Acknowledge this report](#)

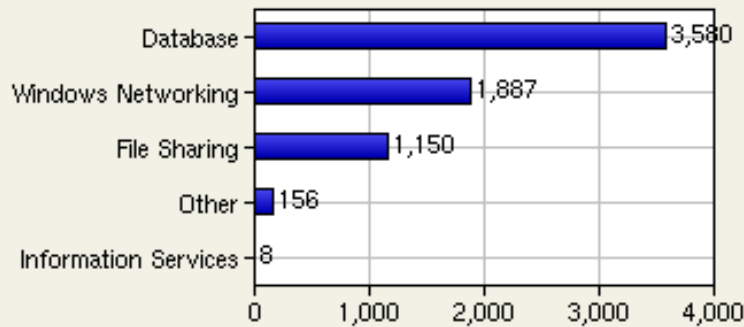
**Attack Summary**



**Informational Events**



**Top Attacked Services**



**Top Attacks**

