

Memorandum

To: Security Service Clients
From: Tom Dedman
Subject: FTP Brute Force Attack in Weekly Summary Report
Date: June 7th, 2010

You may have noticed on today's weekly system summary report for the period of May 31st through June 7th contained a large number of attacks that were identified as not being blocked.

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. In this particular case, CUsource staff determined that these were "Brute Force" attempts to log into our FTP server and did not require immediate correspondence with the owners of the targeted sites.

If you are concerned about this sharp increase and are wondering if any action on your part is required, be assured, no action is needed. As hackers and spammers get more and more sophisticated and prolific, you will continue to see increased numbers of attacks on your weekly reports. If there is reason to be concerned, CUsource staff will contact you immediately, outside your weekly report.

Since the number of "not blocked" attacks associated with these days is so large, we wanted to share more information with each of you so that you can, in turn share with your own board of directors or regulators as you see the need.

The attacks identified in last week's report are what the industry terms a 'brute force' attack against the CUsource FTP service running on the servers that hosts the web pages for many of our 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.

You might recall that a similar event occurred earlier this year, and that these attacks originated from foreign IP addresses. As a result we have shut down access to our web server from any IP address that is not a part of the allocated range of addresses for the continental United States. Last week's login attempts came from networks residing within the U.S.

In response, CUsource staff blocked all FTP access from the networks that these source addresses belonged to at our perimeter last Thursday. We have also conducted a thorough review of the FTP connection logs and have confirmed that all of the connection attempts failed to allow access to the targeted sites.

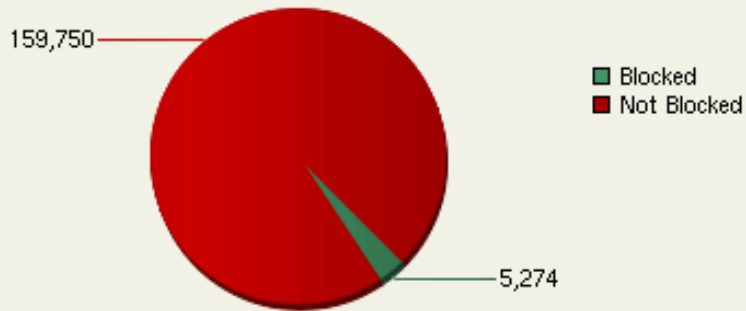
We are also reviewing the potential impact against the benefits of eliminating access to this server to everyone but specifically allowed addresses. This would require that anyone logging onto their site must do so from a static IP address, which could be a hardship for some of our clients. As we determine the best course of action we will be corresponding with anyone who could be impacted.

The attached two pages contain a copy of the weekly summary report and a copy of the detail information regarding the targeted sites and source network. Should you have additional questions regarding this information, please feel free to give me a call at your convenience. We appreciate your business and will continue to protect your system.

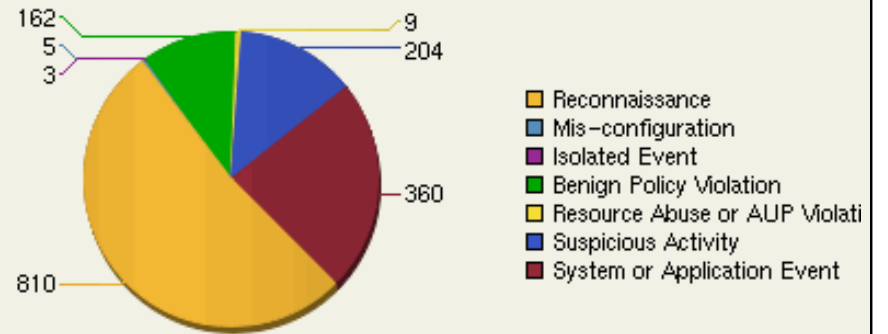
Title Executive Summary: iSensor F-06667, iSensor_F-05300 Group
Subtitle Executive Summary for Mon May 31 2010 - Mon Jun 07 2010
Inspector CUSource, LLC.

[Acknowledge this report](#)

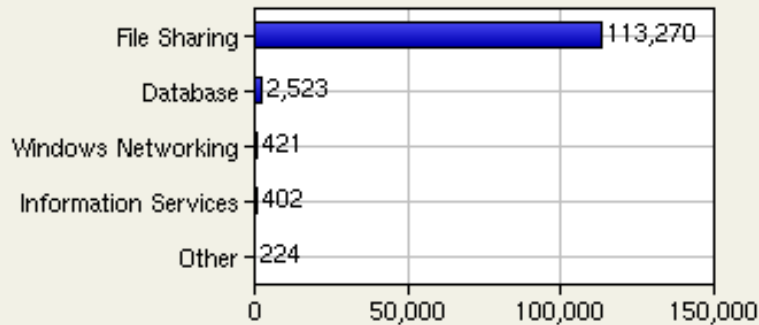
Attack Summary



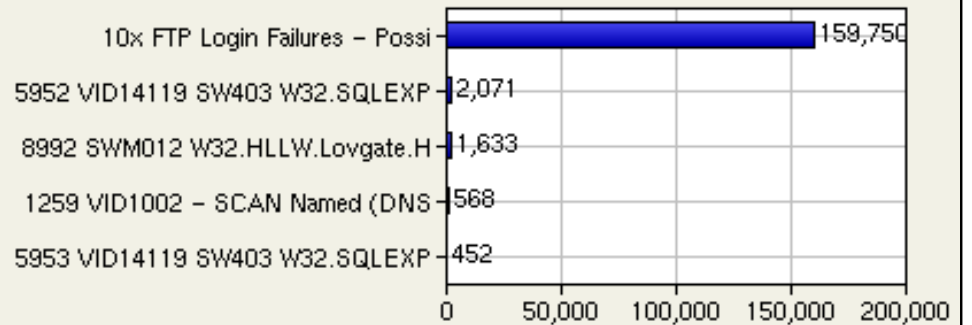
Informational Events



Top Attacked Services



Top Attacks



Date/Time	Severity	Event Id	Event Summary	Action	Incident ID	SrcIp	Source Domain	DstIp	Destination Domain	Count
Wed Jun 02 12:18:20 2010	Medium	30726055	10x FTP Login Failures - Possible Brute Force	Not Blocked	322179	174.37.138.217	softlayer Technologies, Inc	208.79.23.2	uniprosystems.net	9580
Wed Jun 02 12:18:20 2010	Medium	30726058	10x FTP Login Failures - Possible Brute Force	Not Blocked	322179	174.37.138.217	softlayer Technologies, Inc	208.79.23.26	energocomm.org	9580
Wed Jun 02 12:18:20 2010	Medium	30726057	10x FTP Login Failures - Possible Brute Force	Not Blocked	322179	174.37.138.217	softlayer Technologies, Inc	208.79.23.8	bearpawcu.org	9520
Wed Jun 02 12:18:20 2010	Medium	30726056	10x FTP Login Failures - Possible Brute Force	Not Blocked	322179	174.37.138.217	softlayer Technologies, Inc	208.79.23.4	affcom.net	9480
Wed Jun 02 12:18:24 2010	Medium	30726059	10x FTP Login Failures - Possible Brute Force	Not Blocked	322179	174.37.138.217	softlayer Technologies, Inc	208.79.23.34	jeffvantine.com	9590
Wed Jun 02 12:18:28 2010	Medium	30726061	10x FTP Login Failures - Possible Brute Force	Not Blocked	322179	174.37.138.217	softlayer Technologies, Inc	208.79.23.47	montanafcu.com	9530
Wed Jun 02 12:18:28 2010	Medium	30726060	10x FTP Login Failures - Possible Brute Force	Not Blocked	322179	174.37.138.217	softlayer Technologies, Inc	208.79.23.45	mlproperties.com	9520
Wed Jun 02 12:18:40 2010	Medium	30726064	10x FTP Login Failures - Possible Brute Force	Not Blocked	322179	174.37.138.217	softlayer Technologies, Inc	208.79.23.74	svhcommunicator.com	9360
Wed Jun 02 12:18:40 2010	Medium	30726063	10x FTP Login Failures - Possible Brute Force	Not Blocked	322179	174.37.138.217	softlayer Technologies, Inc	208.79.23.70	unused	9540
Wed Jun 02 12:18:40 2010	Medium	30726062	10x FTP Login Failures - Possible Brute Force	Not Blocked	322179	174.37.138.217	softlayer Technologies, Inc	208.79.23.66	services.uniprosystem.net	14620
Wed Jun 02 12:18:44 2010	Medium	30726065	10x FTP Login Failures - Possible Brute Force	Not Blocked	322179	174.37.138.217	softlayer Technologies, Inc	208.79.23.86	richlandfcu.com	15480
Wed Jun 02 12:18:48 2010	Medium	30726066	10x FTP Login Failures - Possible Brute Force	Not Blocked	322179	174.37.138.217	softlayer Technologies, Inc	208.79.23.90	board.bearpawcu.org	9540
Wed Jun 02 12:21:33 2010	Medium	30726160	10x FTP Login Failures - Possible Brute Force	Not Blocked	322179	174.37.138.217	softlayer Technologies, Inc	208.79.23.177	Base IP for LINUX Web	10240
Wed Jun 02 12:21:36 2010	Medium	30726161	10x FTP Login Failures - Possible Brute Force	Not Blocked	322179	174.37.138.217	softlayer Technologies, Inc	208.79.23.179	skyfcu.org	10270
Wed Jun 02 12:21:41 2010	Medium	30726162	10x FTP Login Failures - Possible Brute Force	Not Blocked	322179	174.37.138.217	softlayer Technologies, Inc	208.79.23.180	unused	10210
Thu Jun 03 01:42:55 2010	Medium	30749221	10x FTP Login Failures - Possible Brute Force	Not Blocked	322419	64.52.15.214	Cypress Communications, Inc	208.79.23.2	uniprosystems.net	3690

159750

OrgName: SoftLayer Technologies Inc.
 OrgID: SOFTL
 Address: 1950 N Stemmons Freeway
 City: Dallas
 StateProv: TX
 PostalCode: 75207
 Country: US

OrgName: Cypress Communications, Inc.
 OrgID: CYPC
 Address: 4 Piedmont Center
 Address: Suite 600
 City: Atlanta
 StateProv: GA
 PostalCode: 30305
 Country: US