

Memorandum

To: Security Service Clients
From: Tom Dedman
Subject: FTP Brute Force Attack in Weekly Summary Report
Date: June 22nd, 2010

The weekly summary report you received yesterday (for the period of June 14th through June 21st) contained a large number of attacks that were identified as not being blocked. CUsource staff has determined that these were another series of “Brute Force” attempts to log into our FTP server and did not require immediate correspondence with the owners of the targeted sites.

As documented in previous ‘Brute Force Attack Weekly Summary Report’ memo’s earlier this month, no additional action on your part is needed at this time. 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 this weekly summary 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 the report are what the industry terms a ‘brute force’ or ‘dictionary’ 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.

This is the third such event to occur this year where the attacks originated from foreign IP addresses. As a result of the earlier attacks, we had attempted to 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. We are discovering that the controlling agency for the assignment of IP addresses for the United States, the American Registry of Internet Numbers (ARIN) has been actively reallocating address ranges both in Europe and in Central and East Asia.

This weekend's event originated from an IP address belonging to the Ministry of Education Computer Center for the country of Taiwan. In response, we immediately blocked all FTP access from the networks that these source addresses belonged to at our perimeter. 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. Additionally, we have uploaded a software update to strengthen the FTP server software from such events.

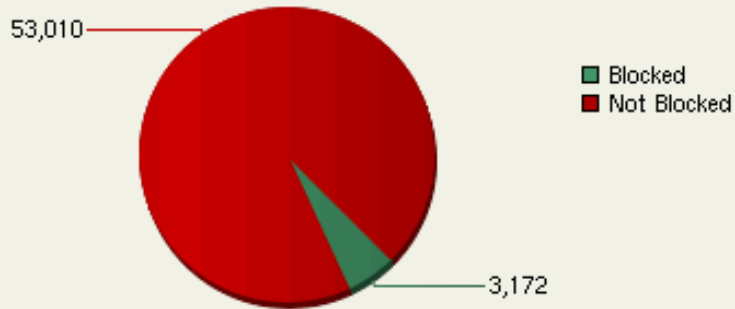
We continue to review the potential impacts of eliminating access to this server to everyone but specifically allowed addresses. This would require that anyone logging onto their site must do so from a static IP address, which could be a hardship for some of our clients. As we determine the best course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

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.

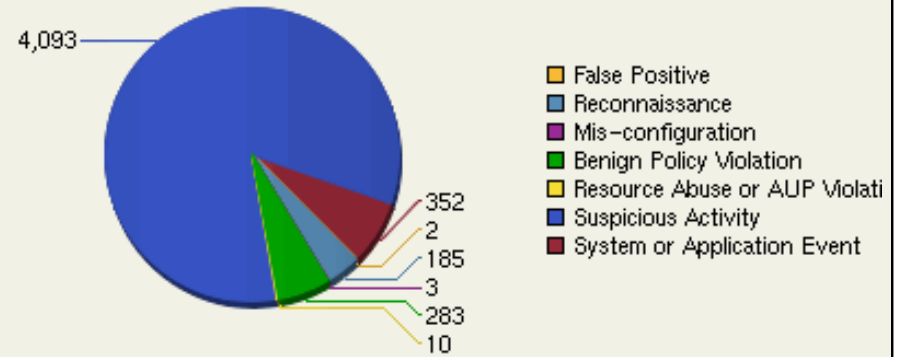
Title Executive Summary: iSensor F-06667, iSensor_F-05300 Group
Subtitle Executive Summary for Mon Jun 14 2010 - Mon Jun 21 2010
Inspector CUSource, LLC.

[Acknowledge this report](#)

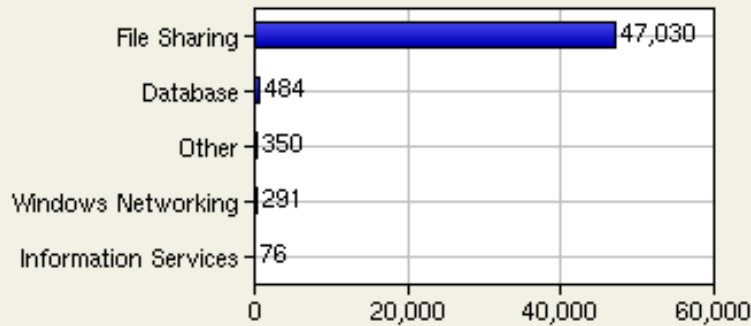
Attack Summary



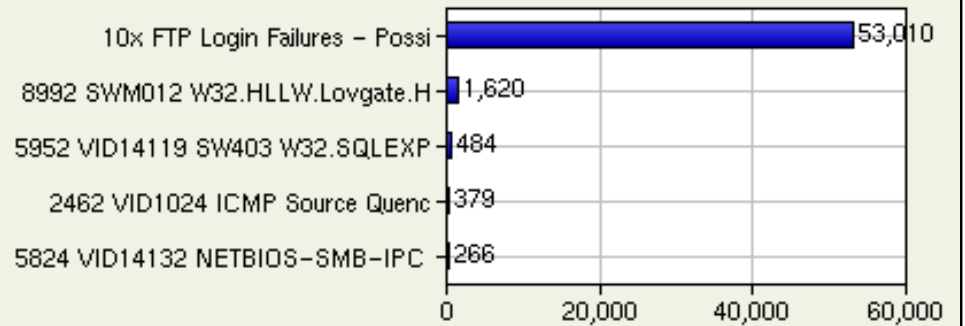
Informational Events



Top Attacked Services



Top Attacks



Content-Type: text/csv

Content-Length: 3512

Content-Disposition: filename="output.csv"

Date/Time	Devlp	Event Id	Event Summary	Action	Incident ID	Srclp	DstIp	Inside IP	WEB Site	Count
Sat Jun 19 17:14:33 2010	iSensor_F-07267/208.79.21.244	31384971	10x FTP Login Failures - Possible Brute Force	Not Blocked	333258	140.114.71.67	208.79.23.4	192.168.2.133	affcom.net	730
Sat Jun 19 17:14:33 2010	iSensor_F-07267/208.79.21.244	31384972	10x FTP Login Failures - Possible Brute Force	Not Blocked	333258	140.114.71.67	208.79.23.2	192.168.2.3	uniprosystems.net	3600
Sat Jun 19 17:14:33 2010	iSensor_F-07267/208.79.21.244	31384973	10x FTP Login Failures - Possible Brute Force	Not Blocked	333258	140.114.71.67	208.79.23.8	192.168.2.143	bearpawcu.org	3620
Sat Jun 19 17:14:37 2010	iSensor_F-07267/208.79.21.244	31384974	10x FTP Login Failures - Possible Brute Force	Not Blocked	333258	140.114.71.67	208.79.23.13	192.168.2.199	Not currently in use	4450
Sat Jun 19 17:14:41 2010	iSensor_F-07267/208.79.21.244	31384975	10x FTP Login Failures - Possible Brute Force	Not Blocked	333258	140.114.71.67	208.79.23.26	192.168.2.148	energcomm.org	3700
Sat Jun 19 17:14:41 2010	iSensor_F-07267/208.79.21.244	31384976	10x FTP Login Failures - Possible Brute Force	Not Blocked	333258	140.114.71.67	208.79.23.34	192.168.2.136	jeffvantine.com	3560
Sat Jun 19 17:14:41 2010	iSensor_F-07267/208.79.21.244	31384977	10x FTP Login Failures - Possible Brute Force	Not Blocked	333258	140.114.71.67	208.79.23.38	192.168.2.197	Linux Web server	4400
Sat Jun 19 17:14:45 2010	iSensor_F-07267/208.79.21.244	31384978	10x FTP Login Failures - Possible Brute Force	Not Blocked	333258	140.114.71.67	208.79.23.45	192.168.2.142	mlproperties.com	3650
Sat Jun 19 17:14:49 2010	iSensor_F-07267/208.79.21.244	31384979	10x FTP Login Failures - Possible Brute Force	Not Blocked	333258	140.114.71.67	208.79.23.47	192.168.2.124	montanafcu.com	3580
Sat Jun 19 17:15:05 2010	iSensor_F-07267/208.79.21.244	31385244	10x FTP Login Failures - Possible Brute Force	Not Blocked	333258	140.114.71.67	208.79.23.71	192.168.2.132	svhcommunicator.com	3600
Sat Jun 19 17:15:05 2010	iSensor_F-07267/208.79.21.244	31385245	10x FTP Login Failures - Possible Brute Force	Not Blocked	333258	140.114.71.67	208.79.23.70	192.168.2.169	Not currently in use	3520
Sat Jun 19 17:15:05 2010	iSensor_F-07267/208.79.21.244	31385246	10x FTP Login Failures - Possible Brute Force	Not Blocked	333258	140.114.71.67	208.79.23.68	192.168.2.150	simpsonhonda.com	3570
Sat Jun 19 17:15:05 2010	iSensor_F-07267/208.79.21.244	31385247	10x FTP Login Failures - Possible Brute Force	Not Blocked	333258	140.114.71.67	208.79.23.66	192.168.2.170	services.uniprosystem.net	4330
Sat Jun 19 17:15:09 2010	iSensor_F-07267/208.79.21.244	31385248	10x FTP Login Failures - Possible Brute Force	Not Blocked	333258	140.114.71.67	208.79.23.73	192.168.2.123	thecu4u.org	3460
Sat Jun 19 17:19:32 2010	iSensor_F-07267/208.79.21.244	31385249	10x FTP Login Failures - Possible Brute Force	Not Blocked	333258	140.114.71.67	208.79.23.74	192.168.2.151	traveltimervs.com	3020
Sat Jun 19 17:38:32 2010	iSensor_F-07267/208.79.21.244	31385683	10x FTP Login Failures - Possible Brute Force	Not Blocked	333258	140.114.71.67	208.79.23.87	192.168.2.186	board.bearpawcu.org	220