

Memorandum

To: Security Service Clients
From: Tom Dedman
Subject: Unblocked attacks in Weekly Summary Reports
Date: April 7th, 2010

As a CUsource Security Service client, you may have noted that the past two weekly system summary reports (March 22nd through March 29th and March 29th through April 5th) contained a large number of attacks that were identified as not being blocked. We were able to immediately identify the source and shut it down.

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, it was simply noted in your weekly reports.

Some of you noted the sharp increase on your reports and contacted the office to see if you needed to do anything else. You do not. We apologize for not communicating this information to you with your weekly reports. 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 this case raised awareness, 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 two weekly reports listed above 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. We allow access via that IP address.

On Saturday, March 27th, more than 60,000 brute force attempts were generated and on Sunday, April 4th an additional 2470 were recorded. The source IP address indicates that these attempts



were all coming from Korea. These attempts were pointed to IP addresses assigned to the web sites as noted on the table shown on page two.

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

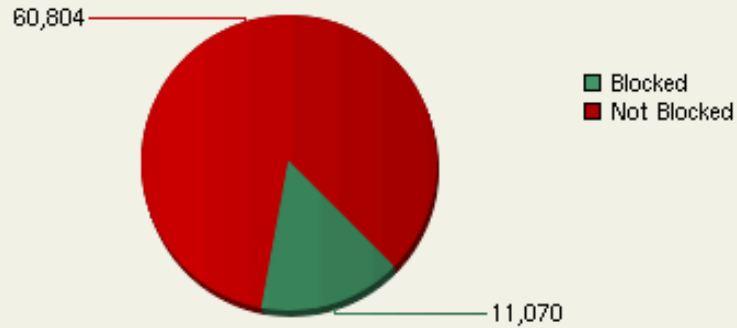
Event Summary	Action	Source IP Address	Target IP Address	Site Name	# of attempts
10x FTP Login Failures - Possible Brute Force	Not Blocked	110.45.144.106	208.79.23.96	WS-ftp server	40
10x FTP Login Failures - Possible Brute Force	Not Blocked	110.45.144.106	208.79.23.96	WS-ftp server	2470
10x FTP Login Failures - Possible Brute Force	Not Blocked	110.45.144.106	208.79.23.2	uniprosystems.net	10
10x FTP Login Failures - Possible Brute Force	Not Blocked	211.236.187.73	208.79.23.19	coop creditunion sites	10
10x FTP Login Failures - Possible Brute Force	Not Blocked	125.138.96.20	208.79.23.15	unassigned	10
10x FTP Login Failures - Possible Brute Force	Not Blocked	125.138.96.20	208.79.23.4	unassigned	10
10x FTP Login Failures - Possible Brute Force	Not Blocked	125.138.96.20	208.79.23.9	familyfirstfcu	10
10x FTP Login Failures - Possible Brute Force	Not Blocked	125.138.96.20	208.79.23.7	richlandfcu	10
10x FTP Login Failures - Possible Brute Force	Not Blocked	125.138.96.20	208.79.23.11	buttecommunityfcu	20
10x FTP Login Failures - Possible Brute Force	Not Blocked	125.138.96.20	208.79.23.6	unassigned	20
10x FTP Login Failures - Possible Brute Force	Not Blocked	125.138.96.20	208.79.23.16	caravithomecare	10
10x FTP Login Failures - Possible Brute Force	Not Blocked	125.138.96.20	208.79.23.18	corporateconsults	10
10x FTP Login Failures - Possible Brute Force	Not Blocked	125.138.96.20	208.79.23.17	communityfcu.org	4330
10x FTP Login Failures - Possible Brute Force	Not Blocked	125.138.96.20	208.79.23.18	corporateconsults	4340
10x FTP Login Failures - Possible Brute Force	Not Blocked	125.138.96.20	208.79.23.10	unassigned	4250
10x FTP Login Failures - Possible Brute Force	Not Blocked	125.138.96.20	208.79.23.11	buttecommunityfcu	4280
10x FTP Login Failures - Possible Brute Force	Not Blocked	125.138.96.20	208.79.23.12	unassigned	4390
10x FTP Login Failures - Possible Brute Force	Not Blocked	125.138.96.20	208.79.23.15	unassigned	4390
10x FTP Login Failures - Possible Brute Force	Not Blocked	125.138.96.20	208.79.23.16	caravithomecare	4340
10x FTP Login Failures - Possible Brute Force	Not Blocked	125.138.96.20	208.79.23.9	familyfirstfcu	4290
10x FTP Login Failures - Possible Brute Force	Not Blocked	125.138.96.20	208.79.23.6	unassigned	4390
10x FTP Login Failures - Possible Brute Force	Not Blocked	125.138.96.20	208.79.23.7	richlandfcu	4340
10x FTP Login Failures - Possible Brute Force	Not Blocked	125.138.96.20	208.79.23.8	bearpawcu	4350
10x FTP Login Failures - Possible Brute Force	Not Blocked	125.138.96.20	208.79.23.3	1stLiberty	4270
10x FTP Login Failures - Possible Brute Force	Not Blocked	125.138.96.20	208.79.23.4	unassigned	4400
10x FTP Login Failures - Possible Brute Force	Not Blocked	125.138.96.20	208.79.23.5	affcomfg	4390
10x FTP Login Failures - Possible Brute Force	Not Blocked	125.138.96.20	208.79.23.2	uniprosystems.net	10
Total					63,390

The following two pages contain the two weekly summary reports I mentioned earlier in this memo. 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.

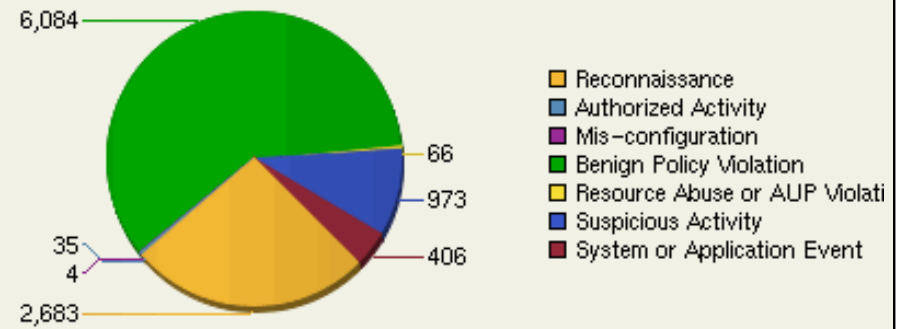
Title Executive Summary: iSensor F-06667, iSensor_F-05300 Group
Subtitle Executive Summary for Mon Mar 22 2010 - Mon Mar 29 2010
Inspector CUSource, LLC.

[Acknowledge this report](#)

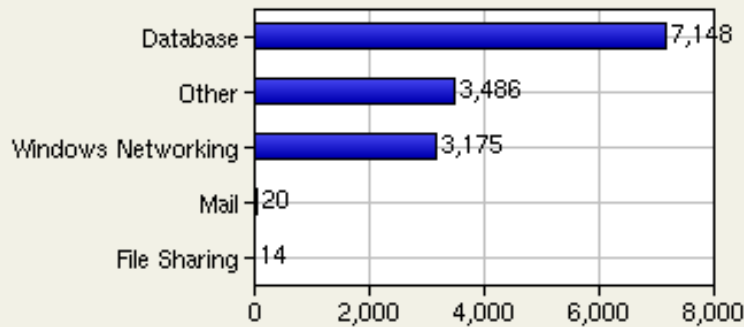
Attack Summary



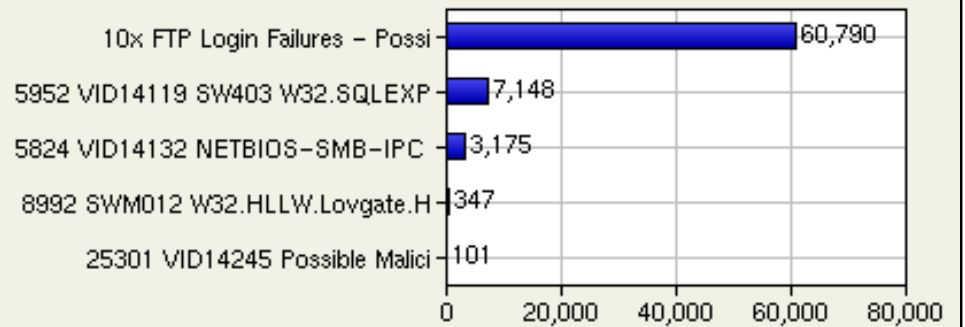
Informational Events



Top Attacked Services



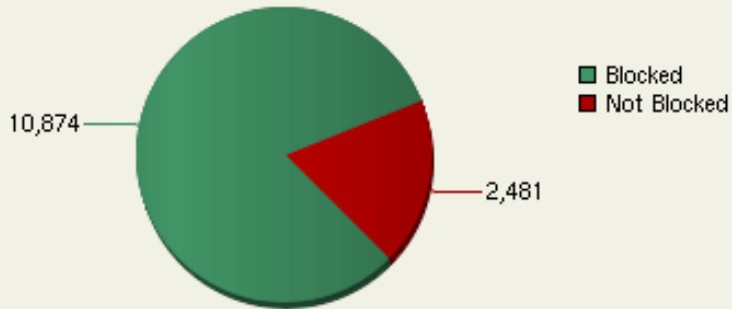
Top Attacks



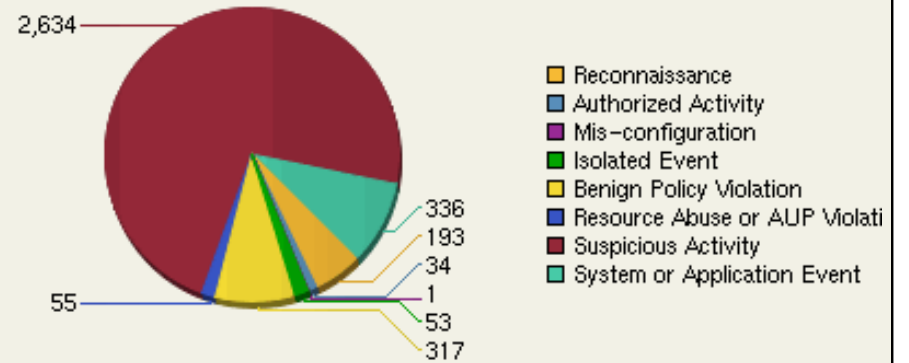
Title Executive Summary: iSensor F-06667, iSensor_F-05300 Group
Subtitle Executive Summary for Mon Mar 29 2010 - Mon Apr 05 2010
Inspector CUSource, LLC.

[Acknowledge this report](#)

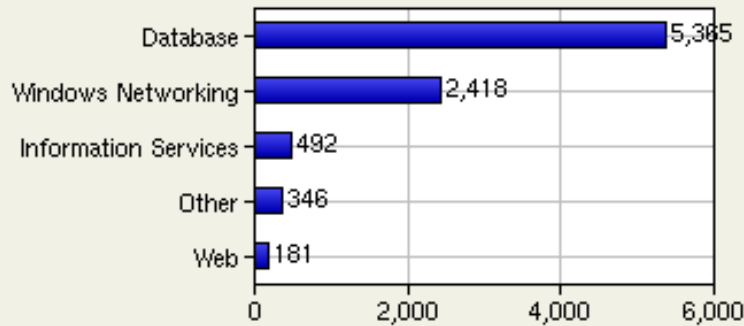
Attack Summary



Informational Events



Top Attacked Services



Top Attacks

