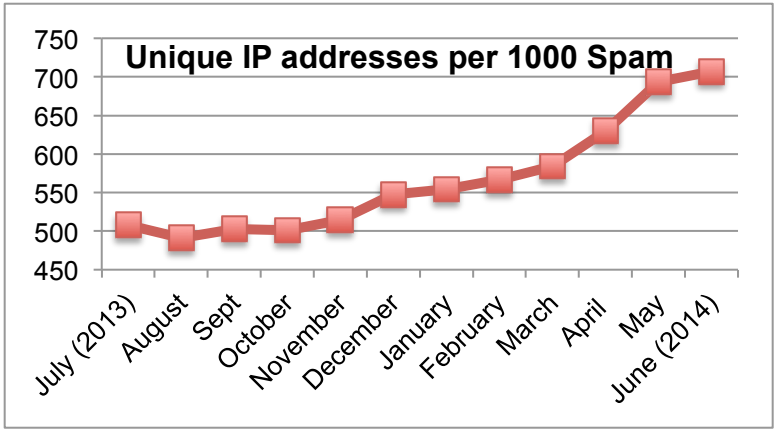
Infographic: "Why Am I Getting More Junk in my Email?"

Recent Increases in Snowshoe Spam and the effect on Email Security Gateway Performance (July/2014)

Joel Snyder, Senior Partner, Opus One

Every modern spam filter uses a combination of techniques to identify unwanted messages. Broadly speaking, these techniques fall into two categories: network-based, and content-based. Network-based anti-spam techniques look at network characteristics, such as IP reputation, without regard to message content; content-based techniques focus on the content of the message, such as checking for malware URLs in the body of a message or a particular combination of words in the subject line. Content-based techniques are also bolstered by other types of spam detection, such as traditional and cloud-based anti-malware detection, URL filtering, and mail-specific techniques such as SPF and DKIM validation.

Reputation services, the most popular network-based anti-spam technique, are used for several reasons: first, they can add a few percentage points to the spam catch rate of a content filter, creating a more effective product. But they have a second benefit in dramatically reducing resources and increasing performance of anti-spam gateways by blocking 60% to 80% (or more) of spam before it even enters the corporate network.

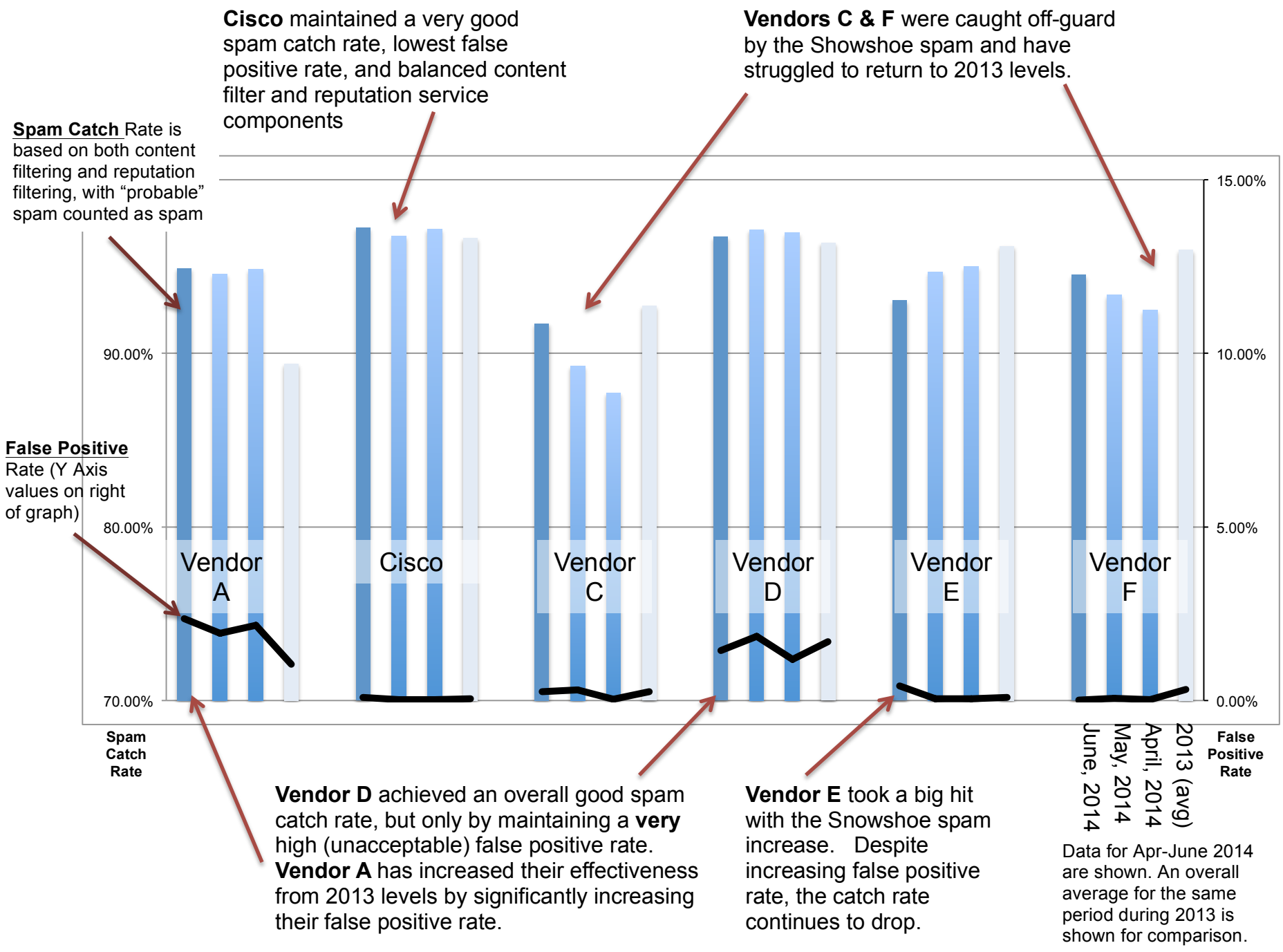


However, the increasing ability to spammers to spread out their footprint across a huge number of IP addresses (so-called "snowshoe spam") has temporarily reduced the effectiveness of reputation services. For example, comparing test results of 48 reputation service scenarios in June 2014, all but one had reduced effectiveness compared to June 2013, by an average of 12 percentage points. The cause of this reduced effectiveness is easy to understand: the huge increase in the number of IP addresses used by spammers. This graph shows the number of unique IP addresses used to send 1,000 spam messages for each of the last twelve months. From July to November 2013, the rate was consistent–about 500 unique IP addresses per 1,000 spam messages. From December 2013 to June 2014, this number increased by nearly 50% to over 700. The "snowshoe" spam burst resulted in reduced effectiveness of many anti-spam gateways, either with increased false positive rate or lower catch rate, or both. Several of the products we test have not yet returned to their 2013 effectiveness levels.

Spammers are constantly changing their techniques to evade filtering. When a product can't effectively respond to these changes, either false positive or false negative (missed spam) rates will jump up. Both results are unacceptable to end users and IT managers.

The increase in "Snowshoe" spam in the last six months highlights **key requirements for enterprise-class anti-spam gateways**: *a high quality content filter* **coupled with** *a high quality reputation service.* Vendors like Cisco who have a good balance have weathered the Snowshoe spam campaigns better than vendors who rely excessively on weaker reputation services or overly aggressive content filters.

Opus One has testied anti-spam solutions on a monthly basis for over 8 years. On the next page, we summarize recent data on products (identified by Gartner as "Leaders" or "Challengers" in their 2014 Magic Quadrant) from our anti-spam testing program. These data show that good anti-spam products have a good balance between content filtering effectiveness, reputation service effectiveness, and false-positive rate. Products that don't balance these three characteristics well are susceptible to noticeable changes in catch or false positive rates during heavy periods of "snowshoe" spam as we have seen in the April/May/June, 2014 time period. Interested readers can review additional multi-vendor product performance in http://www.opus1.com/www/whitepapers/antispamresults2013.pdf for calendar year 2013.


Cisco maintained a very good spam catch rate, lowest false positive rate, and balanced content filter and reputation service components
Vendors C & F were caught off-guard by the Showshoe spam and have struggled to return to 2013 levels.
Spam Catch Rate is based on both content filtering and reputation filtering, with "probable" spam counted as spam
False Positive Rate (Y Axis values on right of graph)
15.00%
10.00%
5.00%
0.00%
90.00%
80.00%
70.00%
Vendor A
Cisco
Vendor C
Vendor D
Vendor E
Vendor F
Spam Catch Rate
False Positive Rate
June, 2014
May, 2014
April, 2014
2013 (avg)
Vendor D achieved an overall good spam catch rate, but only by maintaining a **very** high (unacceptable) false positive rate. **Vendor A** has increased their effectiveness from 2013 levels by significantly increasing their false positive rate.
Vendor E took a big hit with the Snowshoe spam increase. Despite increasing false positive rate, the catch rate continues to drop.
Data for Apr-June 2014 are shown. An overall average for the same period during 2013 is shown for comparison.