Cisco 4Q10
Global Threat Report

Featuring data from four core segments of Cisco Security: Intrusion Prevention System (IPS), IronPort, Remote Management Services (RMS), and ScanSafe.

Key Highlights

- The rate of web malware encounters peaked in October 2010, at 250 average encounters per enterprise for the month;
- Web malware grew by 139 percent in 2010 compared to 2009;
- Search engine-related traffic resulted in approximately 8 percent of web malware encountered in 4Q10;
- Malicious webmail resulted in only 1 percent of web malware encounters for the quarter;
- Rustock botnet activity peaked during the first two weeks of December;
- Legacy worms such as Conficker, MyDoom, Nachi, and Slammer continue to circulate;
- Users flocked to BitTorrent in the wake of the WikiLeaks.org shutdown;
- Global spam levels decreased dramatically in the fourth quarter, following a trend that started in August 2010.

Introduction

The proper security tools can prevent infection or stop outbreaks, mitigate or reduce losses from malicious events, and even decrease legal liability. But these products can also often serve as an excellent source of information about what is happening in your specific enterprise. Regular review and understanding of the logs produced by these tools and services can help you to benchmark what is normal and typical for your enterprise, which in turn provides a benchmark to spot unusual or atypical behavior that might be indicative of an advanced persistent threat or other intrusion.

Correlating log information across various tools and services also provides a timely "pulse" of the threat landscape, which can sometimes have interesting tie-ins to global non-malware-related events. Most importantly, regular review and understanding of the data can help ferret out the elusive "black swan"-the types of surreptitious and malicious events that otherwise could fly below the radar. An excellent example of this was illustrated in the *Cisco 3Q10 Global Threat Report* which showcased the tell-tale signs of a Stuxnet intrusion discoverable via log analysis.

The *Cisco Global Threat Report* is a compilation of data collected across four core segments of Cisco Security: Intrusion Prevention System (IPS), IronPort, Remote Management Services (RMS), and ScanSafe. The report is published quarterly in the hopes that it will inspire and motivate you to perform your own in-house analysis on an ongoing basis.

Contributors to the *Cisco Global Threat Report* include:

Gregg Conklin
Raymond Durant
John Klein
Mary Landesman
Shiva Persaud
Tom Schoellhammer
Chad Skipper
Ashley Smith
Henry Stern

Cisco ScanSafe: Web Malware Events

Enterprise users experienced an average of 135 web malware encounters per month in 2010, with the highest number of encounters (250 per month) occurring in October 2010. At 16,905, the number of unique web malware hosts was also highest in October.

Collectively, there were a total of 38,811 unique web malware hosts resulting in 127,622 unique web malware URLs in the fourth quarter of 2010.

Figure 1 Average Web Encounters per Enterprise, 2010

Source: Cisco ScanSafe

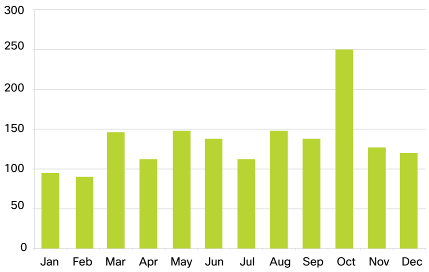


Figure 2 Unique Web Hosts, 2010

Source: Cisco ScanSafe

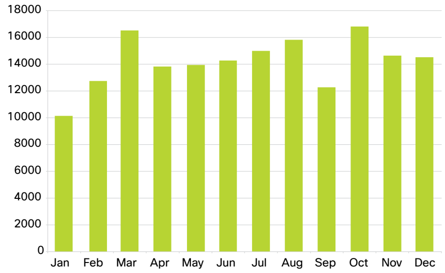
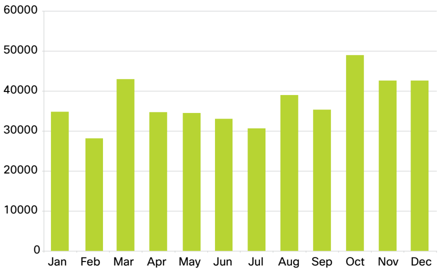


Figure 3 Unique Web Malware URLs, 2010

Source: Cisco ScanSafe

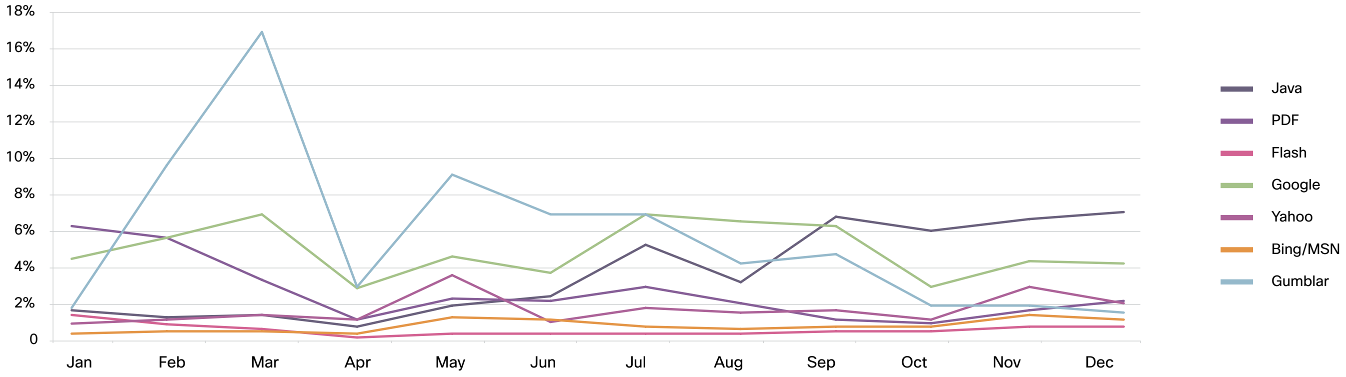


Search engine-related traffic resulted in approximately 8 percent of web malware encountered in the fourth quarter, with the majority occurring from Google (3.84 percent). The 3.84 percent quarterly average represents a remarkable decline; in the third quarter, Google search referrers resulted in 7 percent of all web malware encounters blocked by Cisco ScanSafe. Collectively, malicious webmail resulted in only 1percent of encounters for the quarter.

Gumblar compromises resulted in an average of 2 percent in 4Q10, down substantially from its 17 percent peak in March 2010. Java exploits continued to outpace all other exploits for the year. At 6.5 percent on average for 4Q10, Java exploits were more than four times higher than exploits involving malicious PDF files.

Figure 4 Gumblar, Search, and Top Exploits, 2010

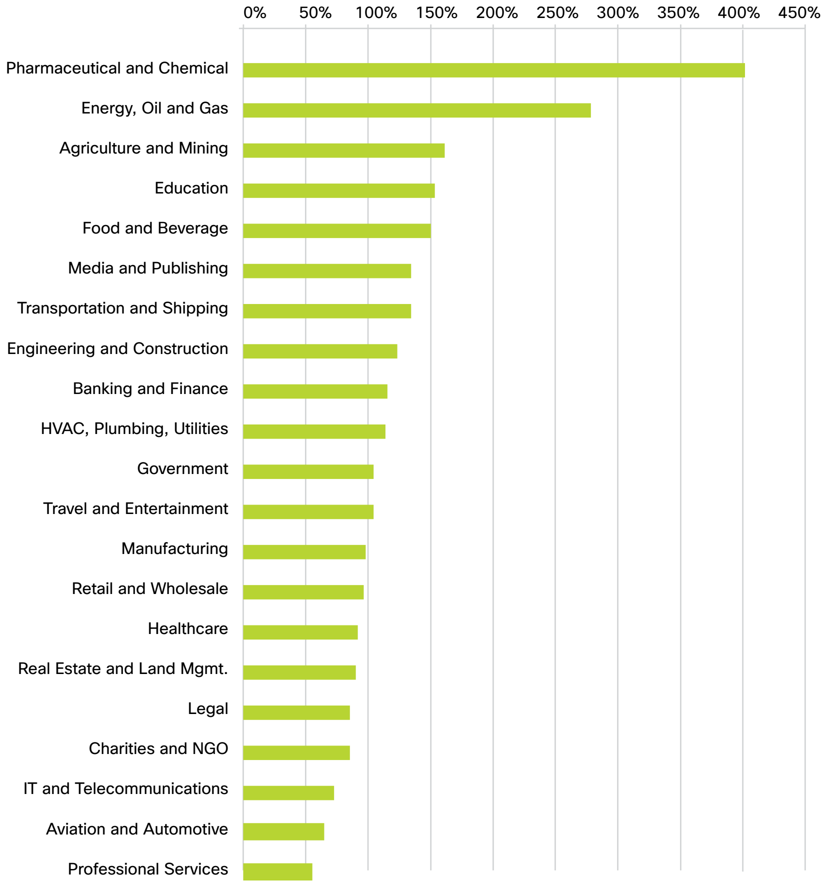
Source: Cisco ScanSafe



Companies in the Pharmaceutical and Chemical and the Energy and Oil sectors continued to be at highest-risk of web malware throughout 2010. Other higher risk verticals throughout the year included Agriculture and Mining, Education, and Food and Beverage. The median rate for all verticals is reflected as 100 percent. Anything above 100 percent has a higher than median encounter rate and anything below 100 percent is below the median for all.

Figure 5 Vertical Risk: Web Malware, 2010

Source: Cisco ScanSafe



Putting It into Focus

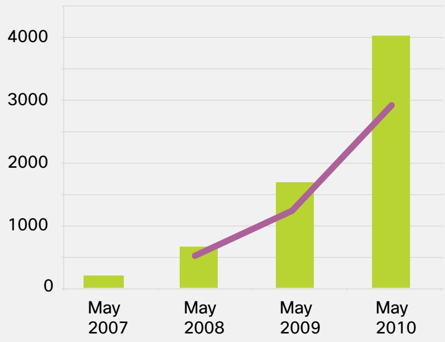
To help explain the impact of web-delivered malware, Cisco ScanSafe tracks a 15,000-seat focus customer's web malware encounters in May of each year. The following chart illustrates in raw numbers the encounters experienced by this focus customer.

It is worth noting that while the rate of encounters has continued to increase dramatically year over year since initial tracking in 2007, the actual rate of increase is declining.

The largest increase, 226 percent, occurred in May 2008 compared to May 2007. The increase in May 2010 compared to May 2009 was significantly less, at 139 percent.

Figure 6 Raw Web Malware Encounters, May YoY

Source: Cisco ScanSafe

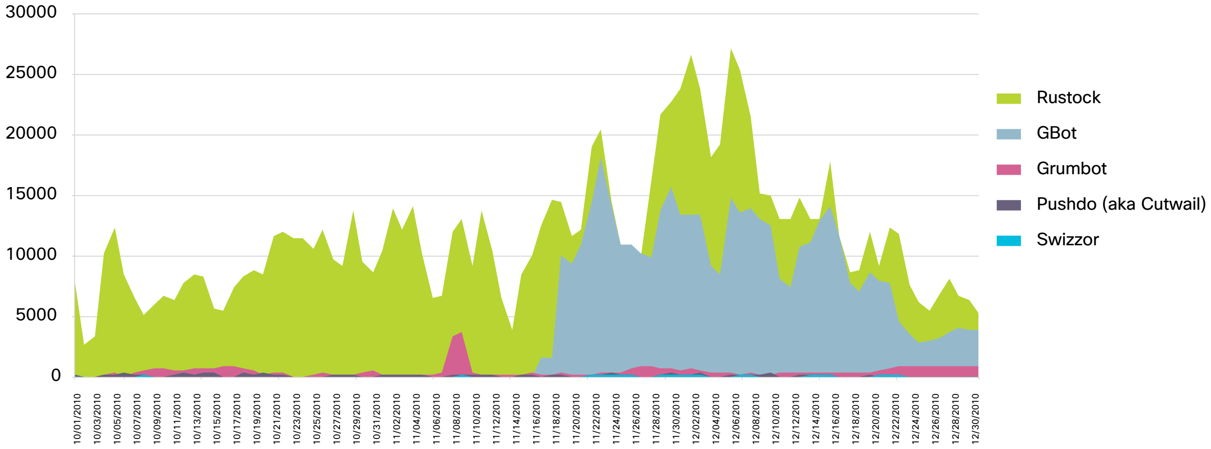


Cisco IPS and RMS: The Inside Threat

Botnet activity plays a role in everything from intellectual property theft to denial of service attacks and spam. Some botnets (such as GBot) wax and wane, while others such as Rustock maintain a steady, pervasive presence. The following chart illustrates botnet activity in 4Q10 for five high-profile bots.

Figure 7 High-Profile Bots, 4Q10

Source: Cisco IPS

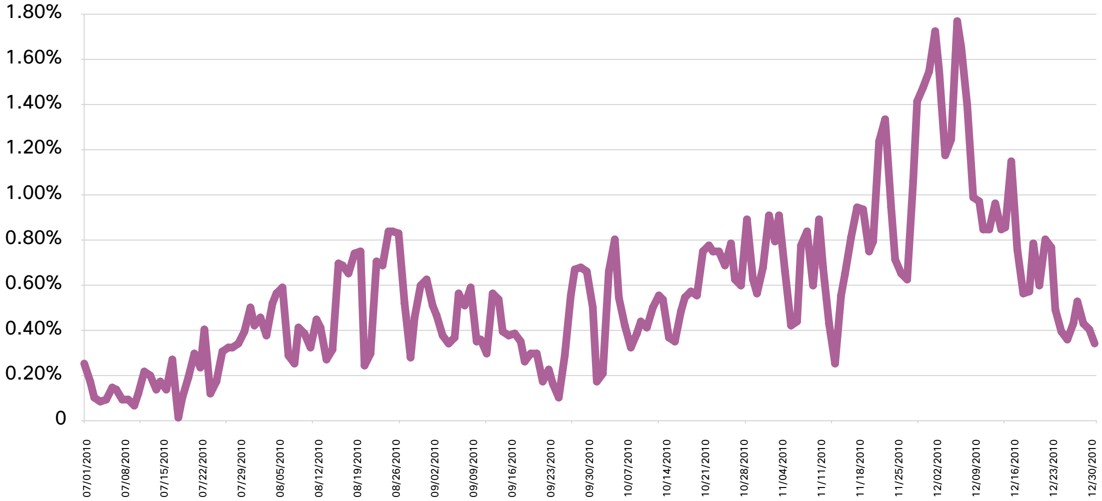


Both Cisco IPS and Cisco RMS for Security observed an upward trend in Gbot botnet activity during the fourth quarter. Gbot command and control traffic is relayed over HTTP rather than using IRC and SSH.

Rustock activity also peaked in the fourth quarter. First discovered in 2006, Rustock installs a rootkit-enabled backdoor that most commonly has been associated with spam and scareware delivery. Figure 8 provides a daily breakdown of Rustock botnet traffic for the second half of 2010.

Figure 8 Rustock Activity, 2H10

Source: Cisco IPS



Following are the top ten IPS signature events recorded by Cisco RMS in 4Q10:

Figure 9 Top 10 Signature Firings, 4Q10
Source: Cisco RMS

Signature	Events
Generic SQL Injection	45.86%
Rustock Botnet	20.05%
WWW WinNT cmd.exe Access	5.16%
Gbot Command and Control Over HTTP	4.73%
Cisco Unified Videoconferencing Remote Command Injection	4.00%
Microsoft Internet Explorer Invalid Flag Reference Remote Code Execution	3.81%
Web View Script Injection Vulnerability	3.02%
B02K-UDP	2.28%
Half-Open Syn	1.57%
TCP Segment Overwrite	0.91%

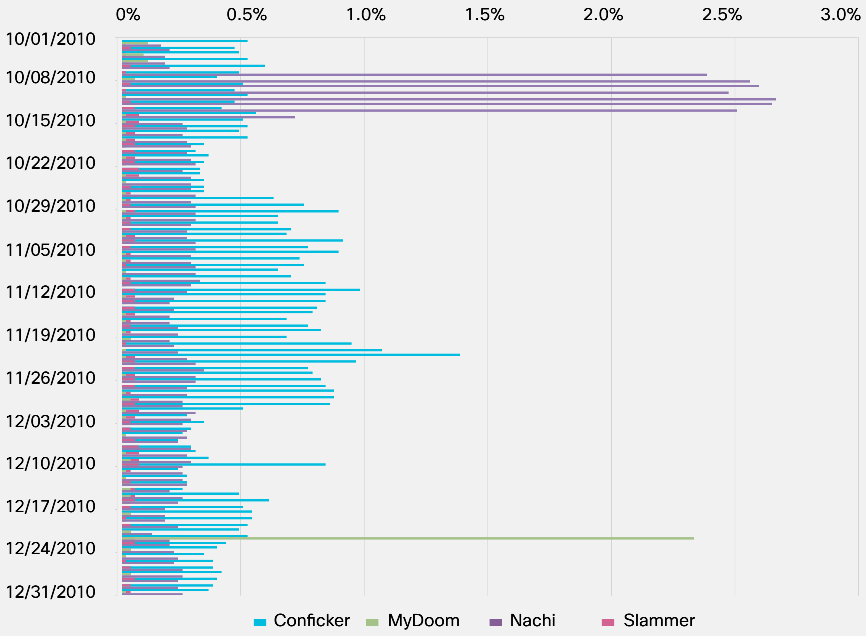
Old Worms Never Die

January 2011 marks the 25th anniversary of Brain (the first PC virus) and the 7th anniversary of MyDoom, one of the most prolific email worms.

While legacy boot sector and DOS file infectors have all but disappeared from the malware scene today, some types of threats, specifically worms, never seem to really die.

To illustrate this point, Cisco IPS gathered signature event data for four older high-profile worms to demonstrate that despite their age, these worms continue to have an impact.

Figure 10 Legacy Worm Activity, 4Q10
Source: Cisco IPS

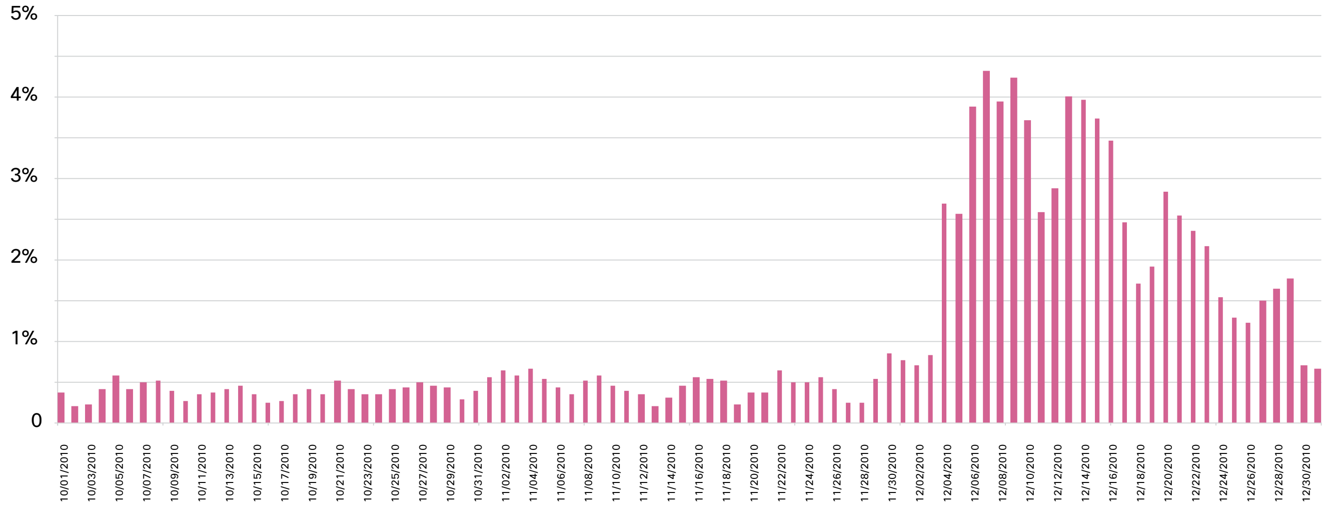


World events also can have an impact on network traffic. One example: the events surrounding WikiLeaks.org subsequent to the site's publishing of classified cables from the U.S. Department of State. When Amazon terminated service to WikiLeaks.org for violations of its terms of service, users flocked to distributed file-sharing networks to obtain copies of the leaked cables.

Figure 11 illustrates BitTorrent activity in 4Q10. Note the steady level of activity through the majority of the quarter, with the sharp and prolonged increase in early December (coinciding with the termination).

Figure 11 BitTorrent Events, 4Q10

Source: Cisco IPS



The following charts depict the ten most active ports observed by Cisco RMS for Security in 4Q10.

Figure 12 External Port Activity, 4Q10

Source: Cisco RMS

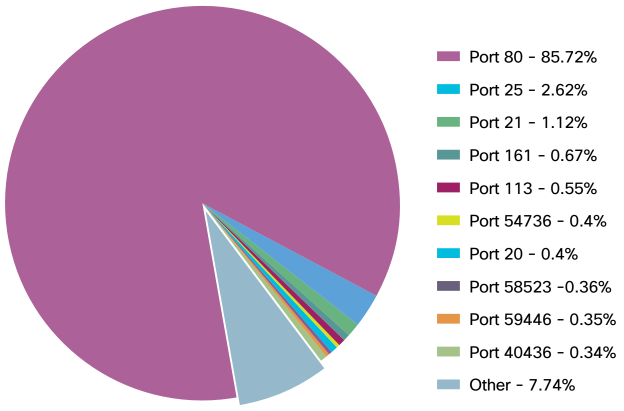
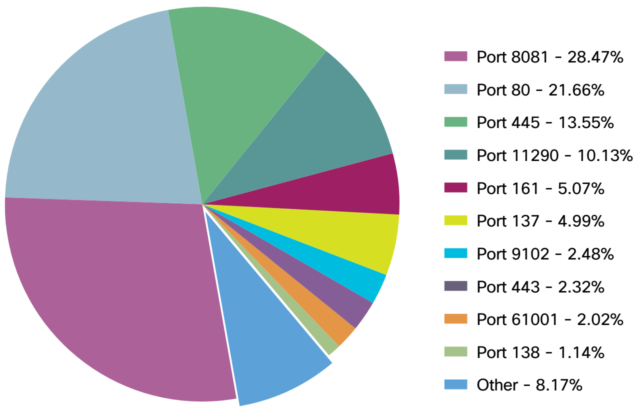


Figure 13 Internal Port Activity, 4Q10

Source: Cisco RMS



Cisco Ironport: Global Spam Trends

Spam volumes dropped considerably in 4Q10, with several key events throughout the year contributing to the decline. Notable events include the takedowns of botnet segments related to Lethic, Waledac, Mariposa, and Zeus in the first quarter, followed by a takedown of a branch of the Pushdo botnet in August 2010. Fourth quarter takedowns included segments of the Bredolab and Koobface botnets.

Also occurring in 4Q10 was the shutdown of SpamIt.org, a facilitating site for spam-related affiliate revenue. The site's closure had a profound impact on pharma-related spam, which until then had been the highest overall category of spam.

Figure 14 illustrates the dramatic impact on spam levels that resulted from these events.

The decline in spam volume was seen globally, as reflected in Figure 15.

Figure 14 Average Daily Spam Volumes by Month, 2010

Source: Cisco IronPort

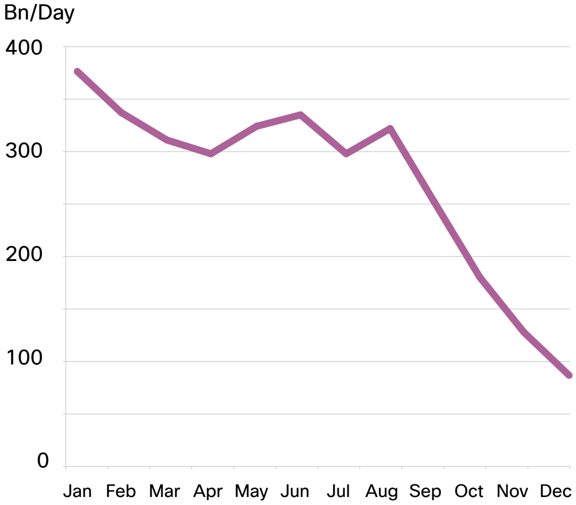
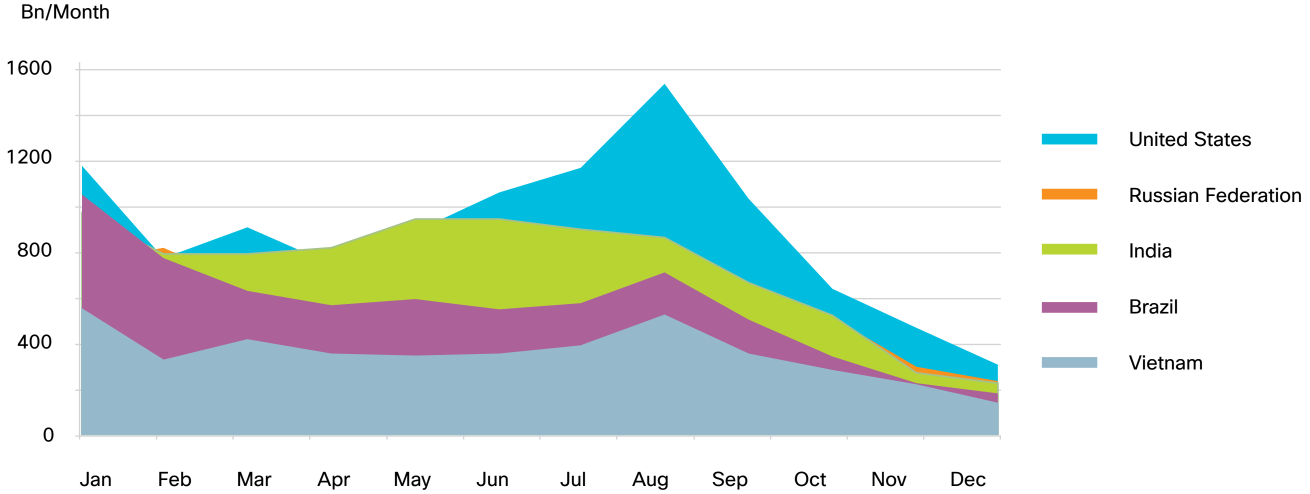


Figure 15 Top Spam Senders by Country, (Bn/Mo), 2010

Source: Cisco IronPort



It's important to note that while spam volumes dropped considerably, attacks via email continued to plague some users. During the Christmas holiday period, an email holiday greeting purporting to be from the White House was sent to .mil and .gov addresses. Those recipients who clicked through to view the "greeting card" were instead greeted by a variant of the Zeus Trojan. This particular variant offloaded DOC, XLS, and PDF files to a remote server. Though quickly discovered, the attackers managed to steal over 2GB of potentially sensitive material.

For more information
on Cisco SIO, visit
www.cisco.com/go/sio.