

A man in a white shirt and patterned tie is looking at a smartphone on a city street. The background is a blurred city street with buildings and trees. A white box is overlaid on the top left of the image, containing the title and subtitle.

Cisco 1Q11 Global Threat Report

Featuring Data from Cisco Security Intelligence Operations

Key Highlights

- 105,536 unique Web malware were encountered in March 2011, a 46% increase from January 2011;
- Malicious webmail represented 7% of all Web-delivered malware in March 2011, a 391% increase from January 2011;
- 45% of all malicious webmail resulted from Yahoo! mail, 25% from Microsoft Live/Hotmail, and only 2% from Google's Gmail;
- Search-engine-related traffic resulted in an average of 9% of all Web malware encountered in 1Q11;
- 33% of search engine encounters were via Google search engine results pages (SERPs), with 4% each from Yahoo! and Bing SERPs;
- SERPs and webmail encounters are impacted by the popularity of a particular service and are likely not indicative of any heightened risk specific to that service;
- Likejacking increased significantly during the first quarter of 2011, from 0.54% of all Web malware encounters in January 2011 to 6% in March 2011;
- At 13%, Miley Cyrus-themed likejacking scams beat out all other celebrities and events in March 2011. Likejacking themes for Indian actress Nayantara were at 7%, while Charlie Sheen was at 3%, Justin Bieber at 2%, and Lady Gaga at 1%;
- At 4% of all Web malware encounters in 1Q11, website compromises that attempted to download the Hiloti Trojan were the most frequently encountered, followed by malicious GIF injections (3%). Website compromises related to the Lizamoon series of SQL injection attacks represented just 0.15% of Web malware encounters for the quarter;
- Though far less successful than in years past, SQL injection attempts continued to be the most prevalent event firing (55%) observed by Cisco Remote Management Services in 1Q11;
- Malware activity related to the MyDoom worm was the 10th most frequently RMS-observed IPS event in 1Q11, demonstrating that legacy malware can still pose a threat to unprotected systems;
- As expected, Rustock activity declined significantly over 1Q11, but, interestingly, the sharp decline commenced weeks prior to the botnet takedown;
- Following 4Q10 declines, global spam volume increased and then subsequently decreased during 1Q11, but levels remained above that of December 2010;
- With an increase of 248%, Indonesia overtook the United States as the top spam-sending country in 1Q11.

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 enable 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: ScanSafe, IPS, RMS, and IronPort. 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:

Jay Chan
Gregg Conklin
Raymond Durant
John Klein
Mary Landesman
Armin Pelkmann
Shiva Persaud
Tom Schoellhammer
Chad Skipper
Ashley Smith

Cisco ScanSafe: Web Malware Events

Enterprise users experienced an average of 274 Web malware encounters per month in 1Q11, a 103% increase compared to 2010. Unique Web malware encountered also increased (46%) in 1Q11, from 72,294 unique Web malware in January 2011 to 105,536 in March (Figures 1-3).

Figure 1 Average Web Encounters per Enterprise, 1Q11

Source: Cisco ScanSafe

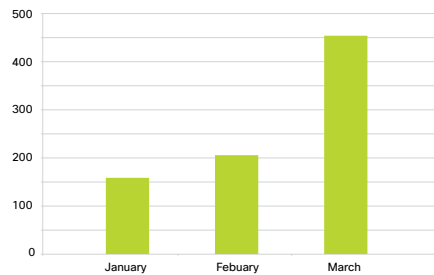


Figure 2 Unique Web Malware Encounters, 1Q11

Source: Cisco ScanSafe

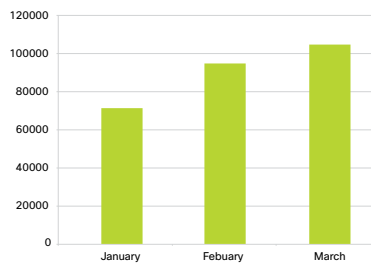
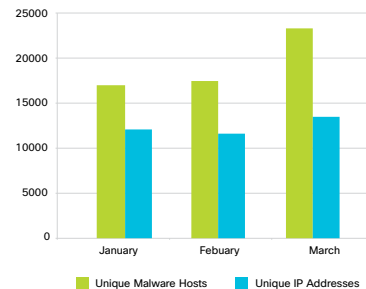


Figure 3 Unique Malware Domains and IPs, 1Q11

Source: Cisco ScanSafe



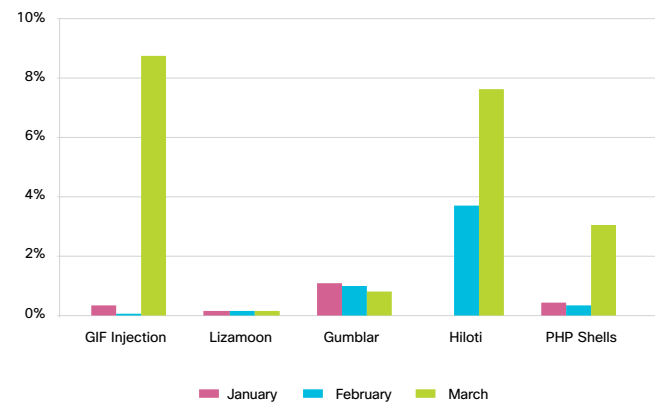
Though Web malware continues to increase, far fewer large-scale compromises are occurring compared to previous years. Instead, compromises are more focused on the “long tail” of the Web, with fewer compromises per attack but a far larger number of separate attacks. As Figure 4 demonstrates, the largest outbreak occurred in March 2011 with a series of GIF injection attacks targeted at popular Pakistani news sites.

The second largest attack in 1Q11 involved website compromises designed to deliver the Hiloti trojan. This particular wave of attacks, breaking in January 2011 before resuming in February, is part of an ongoing series.

Though the Lizamoon series of SQL injection attacks were highly publicized in March 2011, both the actual numbers of compromised websites and the live encounter rates were far fewer than had been reported. In reality, only a few thousand websites were actually compromised and live encounters represented only 0.15% of all Web malware encountered for the quarter.

Figure 4 High Profile Web Attacks, 1Q11

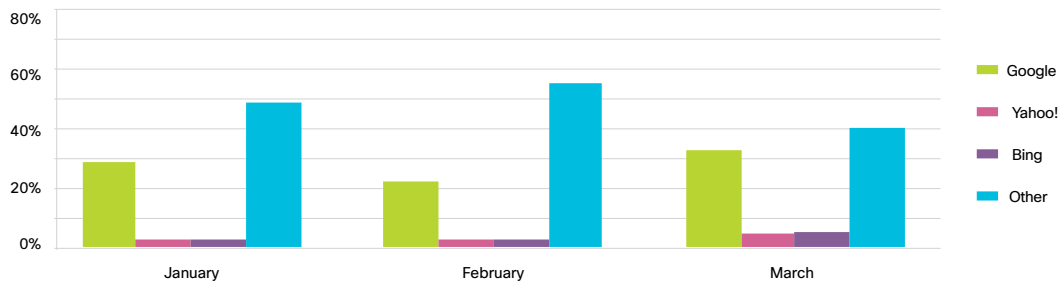
Source: Cisco ScanSafe



Web searches resulted in 9% of Web malware encounters in 1Q11, with an average of 33% resulting from Google search engine results pages (SERPs) and 4% each from Yahoo! and Microsoft Bing SERPs. The majority of Web search encounters (58%) occurred via smaller search engines and/or searches performed on non-search-engine websites (Figure 5).

Figure 5 Search Engine Web Malware Encounters, 1Q11

Source: Cisco ScanSafe



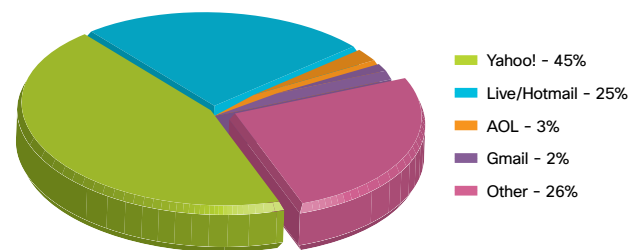
It is important to note that search-related malware encounters are not reflective of any underlying risk with a particular search engine; rather, these encounters are due to the popularity and thus increased usage of a particular search service.

The rate of malware encounters via webmail increased rather dramatically in 1Q11, from 1% of all Web malware encounters in January 2011 to 7% in March 2011.

The majority of all 1Q11 malicious webmail (44%) occurred via Yahoo! mail (Figure 6). As with search engine encounters, webmail encounter rates are likely more reflective of the popularity of a given webmail service rather than specific to any elevated (or reduced) risk.

Figure 6 Webmail Malware Encounters, 1Q11

Source: Cisco ScanSafe



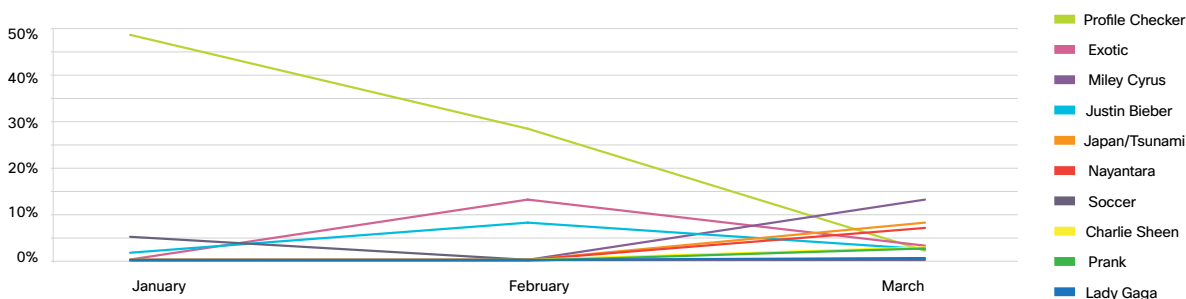
“Likejacking” refers to a method of clickjacking that uses image overlays to forcibly cause a Facebook user to “Like” a particular page. In turn, this causes a link to the page to appear on the user’s Facebook wall, exposing their Facebook friends to the likejacking scam. This worm-like scam is often accompanied by a phishing segment whereby the victim is also tricked into providing their Facebook username and password.

As shown in Figure 7, likejacking encounters increased significantly during 1Q11, from 0.54% of all Web malware in January 2011 to 6% in March 2011. At 48%, the most frequently encountered “hook” for likejacking scams in January 2011 involved claims that the link would enable the victim to see who had been viewing their profile. However, this scam declined in effectiveness throughout the quarter, resulting in only 2% of likejacking encounters in March 2011.

Among celebrities, Miley Cyrus-themed likejacking dominated, with 13% of all likejacking encounters in March 2011. The second highest celebrity-themed likejacking leveraged the popularity of Indian actress Nayantara, resulting in 7% of likejacking scams for the same month.

Figure 7 Top 10 Likejacking Scams, 1Q11

Source: Cisco ScanSafe

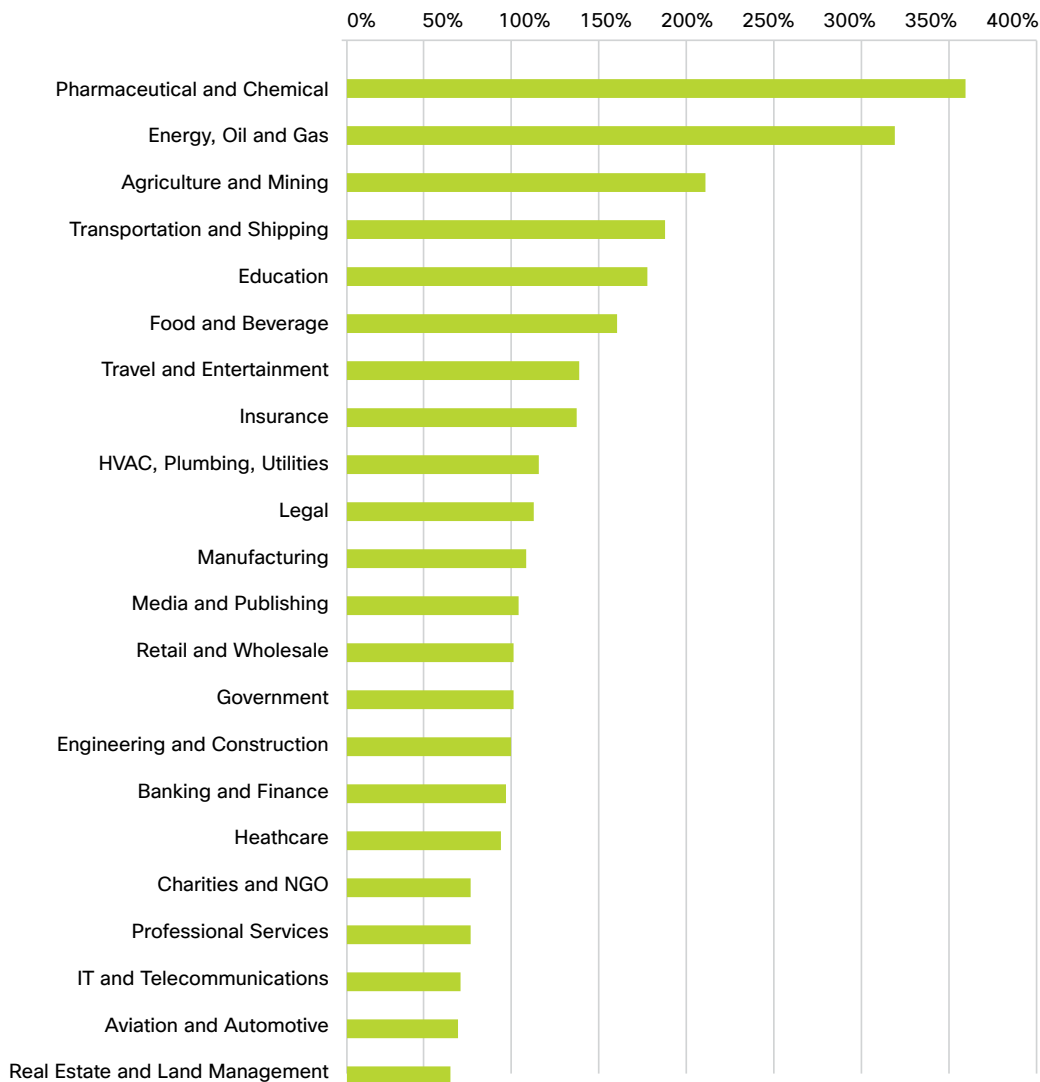


At 5% of all Web malware encounters, Java exploits continued to outpace Adobe Reader and Acrobat exploits (1%), as well as Adobe Flash exploits (0.17%), in 1Q11.

Companies in the Pharmaceutical & Chemical and the Energy & Oil sectors continued to be at highest risk of Web malware throughout 1Q11. Other higher-risk verticals throughout the quarter included Agriculture & Mining, Transportation & Shipping, and Education. The median rate for all verticals is reflected as 100%—anything above 100% has a higher-than-median encounter rate, and anything below 100% is below the median for all (Figure 8).

Figure 8 Vertical Risk, 1Q11

Source: Cisco ScanSafe



Cisco IPS and Remote Management Services

As discussed in the Cisco 4Q10 Global Threat Report, legacy worm activity continues to have an impact—even years after protection against the malware has been made readily available. That trend continues in 2011 with the surprise appearance of the circa-2004 MyDoom worm in the top 10 IPS event firings observed by Cisco Remote Management Services during the first quarter (Figure 9).

Figure 9 Top 10 Signature Firings, 1Q11

Source: Cisco RMS

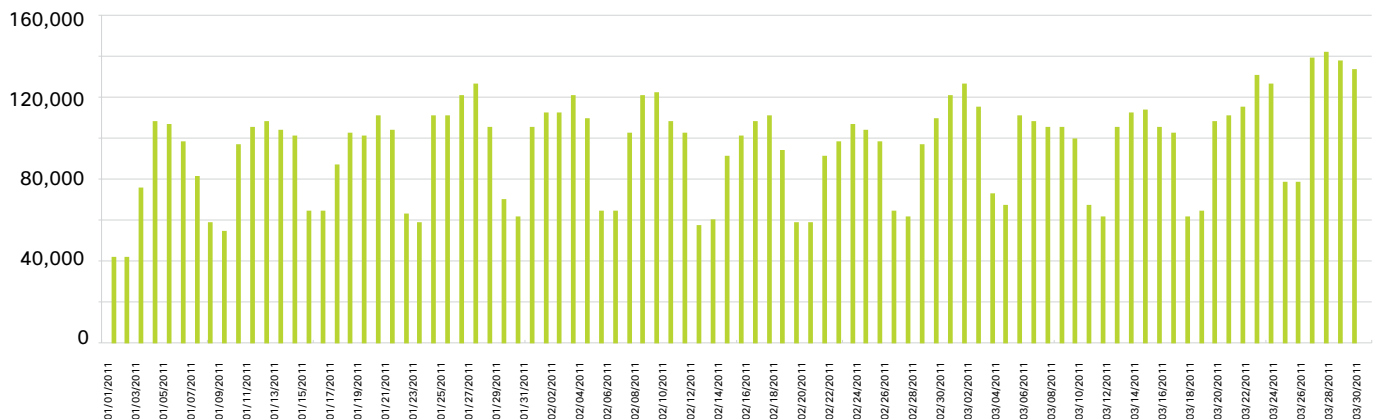
Signature	Events
Generic SQL Injection	55.03%
Web View Script Injection Vulnerability	7.01%
Gbot Command and Control Over HTTP	5.16%
B02K-UDP	5.20%
Cisco Unified Videoconferencing Remote Command Injection	4.91%
Microsoft Internet Explorer Invalid Flag Reference Remote Code Execution	3.27%
Windows MHTML Protocol Handler Script Execution	2.47%
WWW WinNT cmd.exe Access	1.30%
Web Application Security Test/Attack	1.19%
MyDoom Virus Activity	1.16%

Note that the MHTML vulnerability described in Microsoft KB 2501696, IntelliShield alert 22310, and Cisco Intrusion Prevention System (IPS) 6.0 - 33379/0 also appears on the Cisco RMS top 10 signature events list for 1Q11. Microsoft released an update for this former zero-day vulnerability in April 2011 (MS11-026).

While a significantly occurring event in 1Q11, SQL injection attempts remained at a fairly steady pace throughout the quarter with the only notable increase occurring in the latter part of March 2011 (Figure 10).

Figure 10 SQL Volume, 1Q11

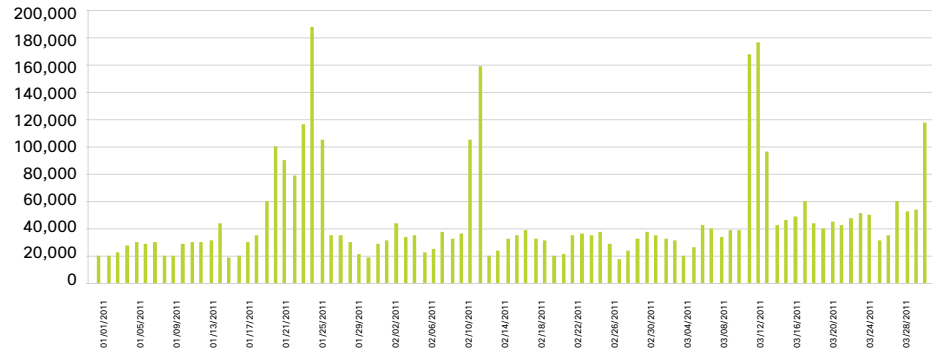
Source: Cisco IPS



Denial-of-Service (DoS) attacks also had a steady presence throughout 1Q11, with several notable peaks occurring throughout the quarter (Figure 11). While once largely prank-related, DoS attacks are increasingly politically and financially motivated.

Figure 11 DoS Volume, 1Q11

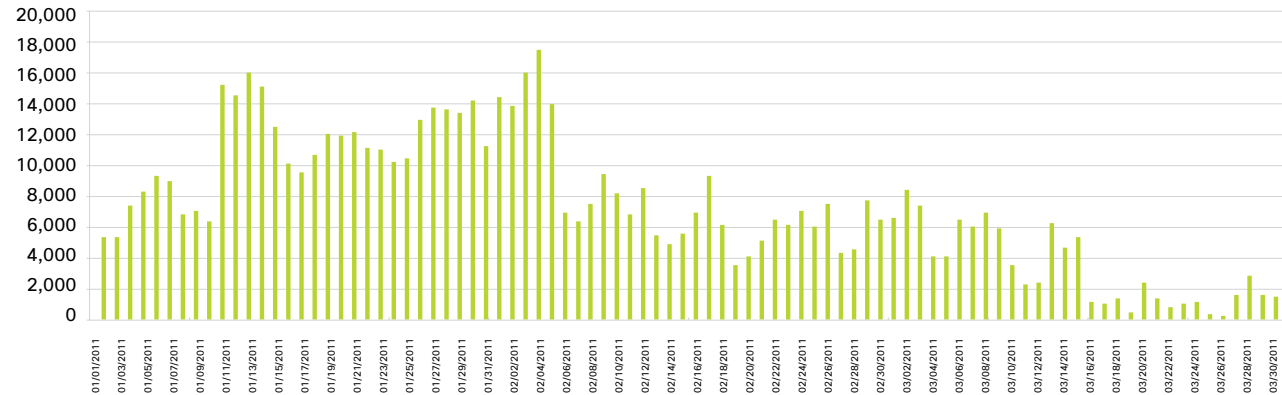
Source: Cisco IPS



Rustock activity, which had peaked in the fourth quarter of 2010, significantly declined in 1Q11. First discovered in 2006, Rustock installs a rootkit-enabled backdoor that has most commonly been associated with spam and scareware delivery. On March 16, 2011, it was reported that global law enforcement and Microsoft had successfully dismantled key segments of the Rustock botnet. However, as seen in Figure 12, Rustock activity had begun to decline several weeks prior to the takedown event.

Figure 12 Rustock Volume, 1Q11

Source: Cisco IPS



Activity, Top 25, 1Q11

Source: Cisco RMS

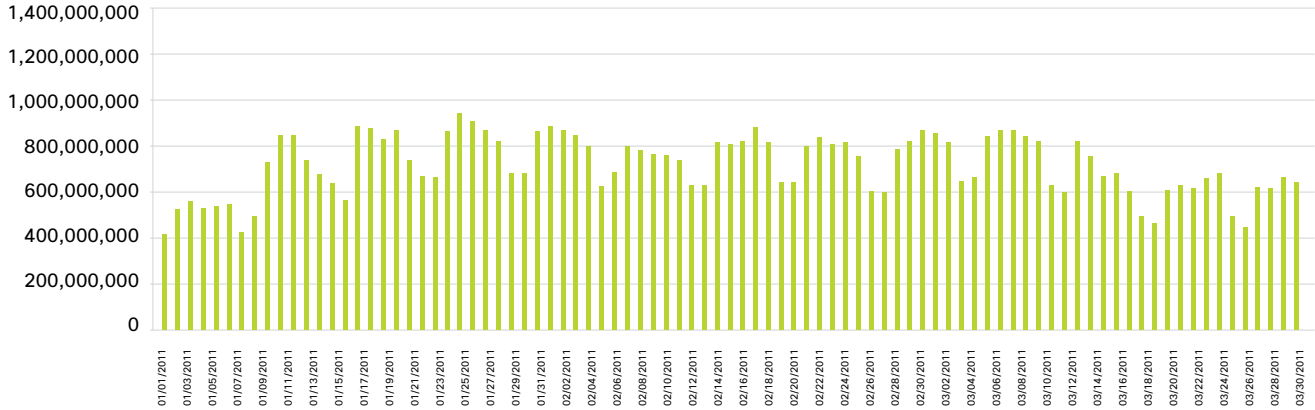
Port	Percent
80	69.00%
40436	2.23%
25	2.17%
161	1.39%
5060	1.27%
123	1.16%
34227	1.13%
443	1.05%
21	1.00%
20	0.71%
554	0.57%
39162	0.47%
59446	0.47%
49688	0.35%
41483	0.25%
29930	0.24%
44122	0.24%
3985	0.20%
445	0.19%
3986	0.19%
57522	0.18%
63650	0.18%
58198	0.18%
53565	0.17%
54826	0.16%

Cisco IronPort: Global Spam Trends

The 2011 takedown of segments of Rustock, combined with multiple spam botnet takedowns in 2010, had a positive impact on overall spam volume. However, spam volume in 1Q11 remained above the lowest point recorded in December 2010. Figure 13 reflects global spam volume as reported through Cisco SensorBase Network participants.

Figure 13 Global Spam Volume, 1Q11

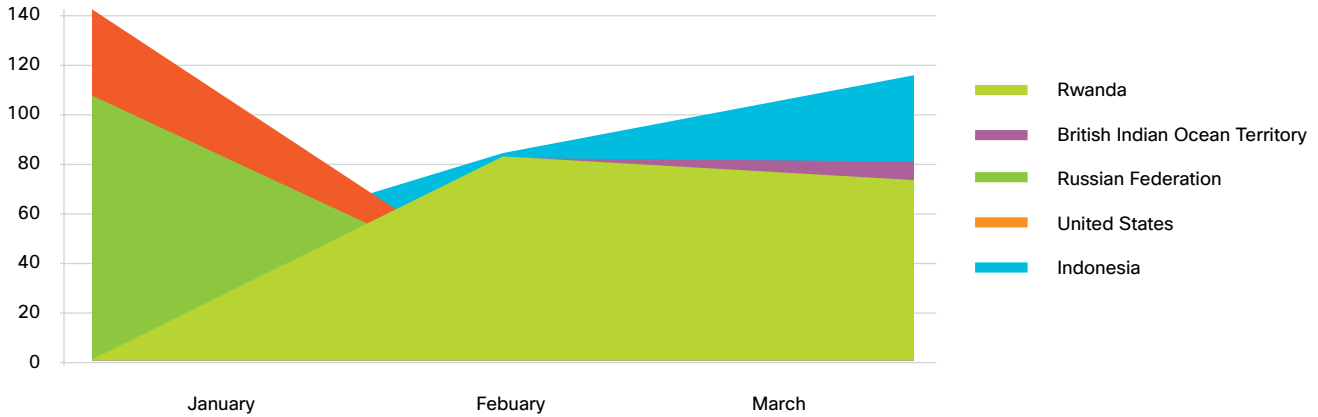
Source: Cisco IronPort (SBNP/ESA)



Interestingly, while the takedown efforts had the most positive impact on spam originating from the United States and Russia, spam originating from other countries is rapidly increasing (Figure 14).

Figure 14 Top Spam Senders by Country, (Bn/Mo), 1Q11

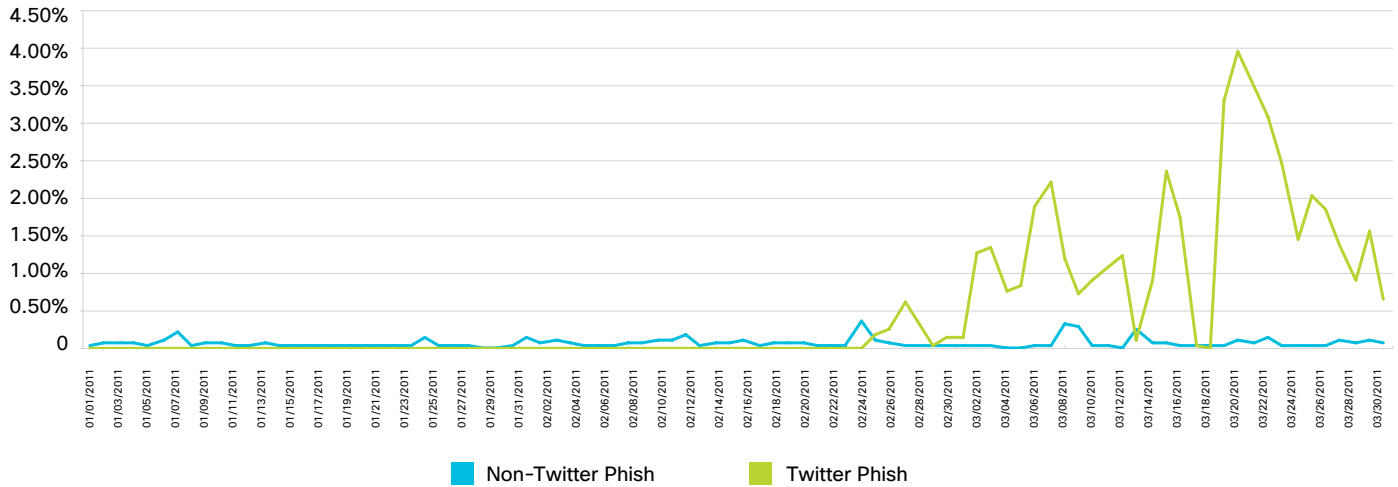
Source: Cisco IronPort



Although they represent a relatively small percentage of overall spam, phishing attacks pose a serious risk to security, both from a financial and sensitive information disclosure perspective. In 1Q11, attackers increasingly turned their attention toward phishing Twitter accounts (Figure 15). This interest in Twitter credentials is likely due in part to Twitter users' acceptance of shortened URLs. By compromising Twitter accounts, attackers can take advantage of shortened URLs to entice followers to visit malicious links the users might ordinarily view as suspicious. Such attacks are further fueled by the trust engendered through social networking in general.

Figure 15 Global Spam Volume, 1Q11

Source: Cisco IronPort (SBNP/ESA)



In summary, while global spam volumes have increased, the malware encounter rate via webmail has substantially increased. Further, social networking scams involving both Facebook and Twitter also increased throughout the first quarter. Web-delivered malware is also at an all-time high and the rate of encounters with unique new malware continues to increase



Americas Headquarters

Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters Cisco

Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters

Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.