Cisco 2Q10 Global Threat Report

Key Highlights

- Eastern Europe encountered the highest rate of web-based malware in 2Q10, followed by South America and China;
- IPS SQL injection signature firings increased substantially in 2Q10, coinciding with outbreaks of SQL-injection-compromised websites;
- Asprox SQL injection attacks made a reappearance in June of 2010, after nearly six months of inactivity;
- Gumblar-compromised websites continued to be the most frequently encountered sources of web-based malware in 2Q10;
- 7.4 percent of all web-based malware encounters in 1Q10 resulted from search engine queries and nearly 90 percent of all Asprox encounters in June of 2010 were the results of links in search engine results pages;
- Companies in the Pharmaceutical and Chemical vertical were the most at risk for web malware encounters, experiencing a heightened risk rating of 400 percent in 1Q10 and 543 percent in 2Q10;
- Increases in peer-to-peer (P2P) activity were observed across the top three P2P networks (eDonkey, Gnutella, and BitTorrent) throughout the first quarter of 2010, with the strongest increase in March of 2010;
- Continuous high saturation in 2Q10, coupled with recent P2P malware developments, suggest that peer-to-peer file shares are becoming increasingly favored by users and malware attackers alike.

Encounter Rates

The number of unique malware hosts and malicious URLs remained fairly constant month-over-month during the second quarter of 2010. This is a significant development in terms of web-based malware, as it marks the first time since tracking began in 2007 that the number of malware hosts and URLs has remained relatively flat over an entire quarter.

Despite the 2Q10 leveling of malicious URLs and malware domains, the average daily encounter rate increased month-over-month throughout the quarter.

Figure 1 **Unique Web-Based Malware Hosts, 1H10**

Source: Cisco ScanSafe

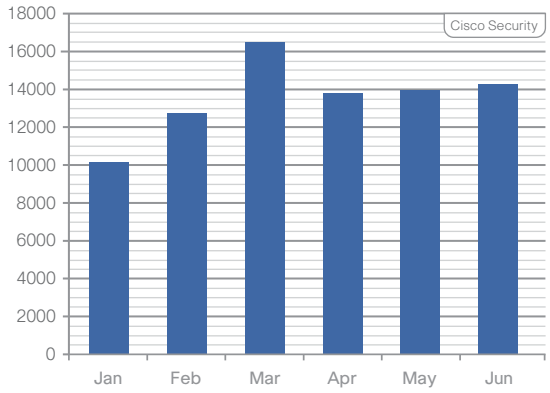
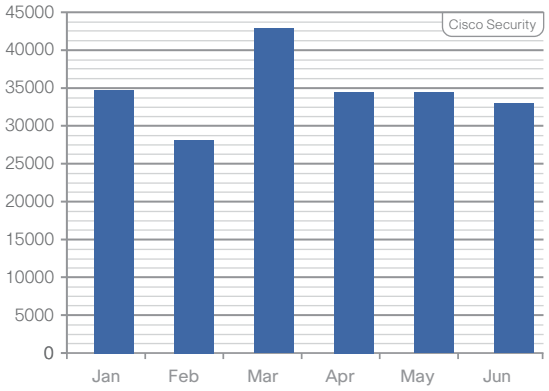


Figure 2 **Unique Web-Based Malware URLs, 1H10**

Source: Cisco ScanSafe



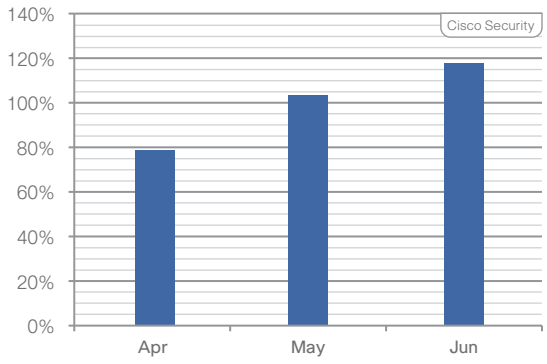
Exploits

65 percent of all web-based malware encounters were blocked prior to exploit code or involved encounters which did not include exploit code. Of exploits that are encountered, those targeting Adobe Reader/Acrobat, Sun Java, and Adobe Flash were the three most common during the first half of 2010.

Unfortunately, exposure is not necessarily a direct result of the quantity of malware hosts/URLs. Instead, the quality of traffic driving efforts (for example, black hat search engine optimization and social engineering) to those malware hosts/URLs bears more of an impact on overall encounter rates.

Figure 3 **Average Daily Encounter Rates, 2Q10**

Source: Cisco ScanSafe



Encounters with web-based malware increased month-over-month in the first quarter with a significant increase in March of 2010. That increase was followed by a drop in encounters in April of 2010— likely the result of a series of concerted takedown efforts from various sources aimed at the Waledac, Mariposa, and Zeus botnets. In June of 2010, the average daily encounter rate had increased to the same level observed in March of 2010.

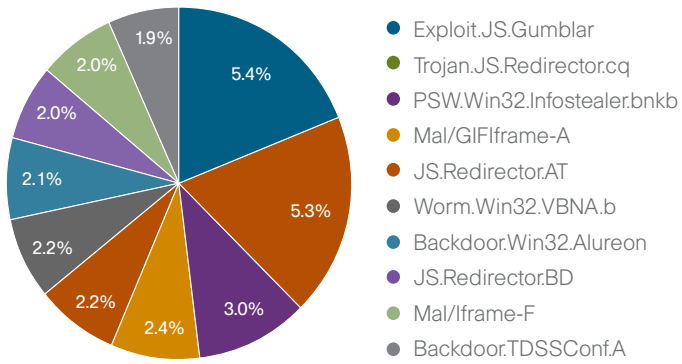
65 percent of all web-based malware encounters were blocked prior to exploit code or involved encounters which did not include exploit code. Of exploits that are encountered, those targeting Adobe Reader/Acrobat, Sun Java, and Adobe Flash were the three most common during the first half of 2010.

Malware Prevalence

Gumblar comprised 5 percent of all web-based malware in 2Q10 and 11 percent of all web-based malware in 1Q10, with the highest concentration during March of 2010 (17 percent).

Figure 4 **Top Ten Web-Based Malware, 2Q10**

Source: Cisco ScanSafe

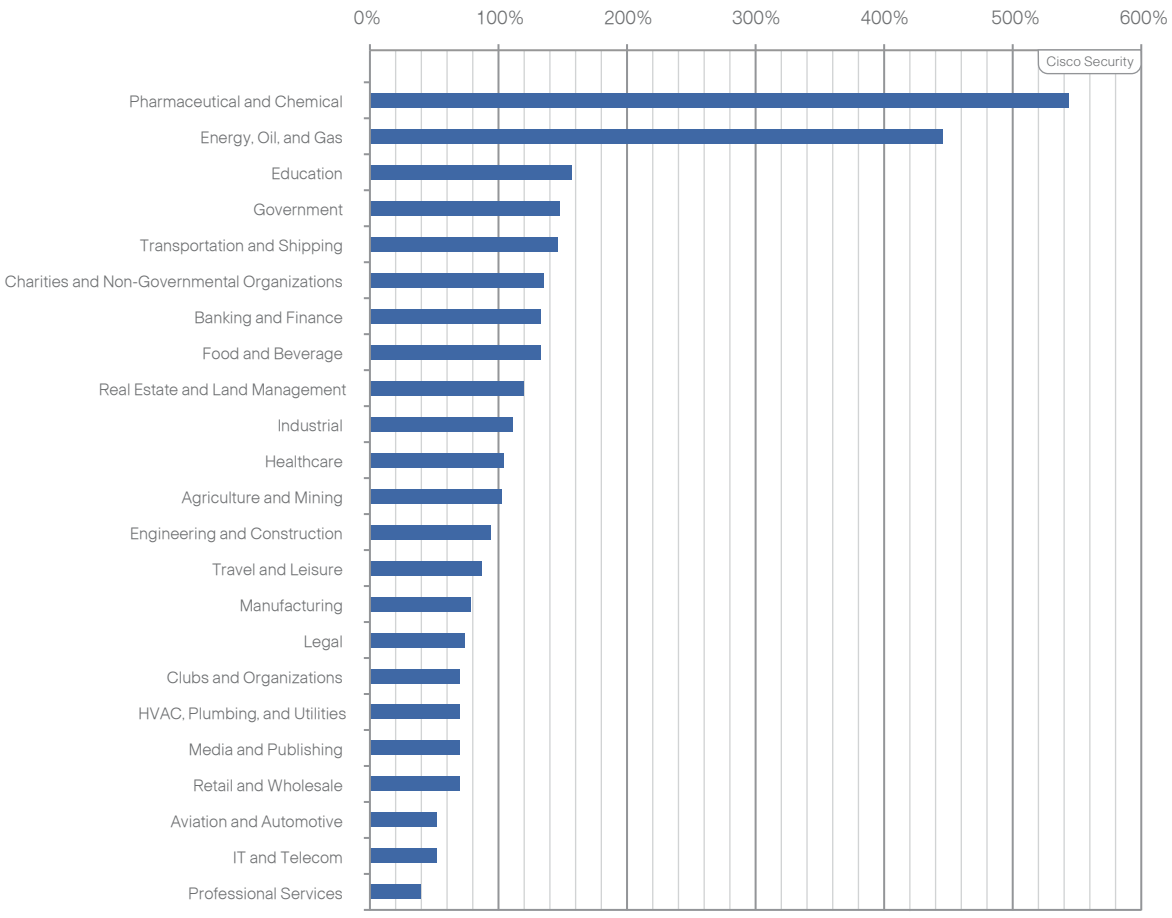


The Vertical Risk

Companies in the Pharmaceutical and Chemical vertical were the most at risk for web-based malware encounters, experiencing a heightened risk rating of 543 percent in 2Q10, up from 400 percent in 1Q10. Other higher risk verticals in 2Q10 included Energy, Oil, and Gas (446 percent), Education (157 percent), Government (148 percent), and Transportation and Shipping (146 percent).

Figure 5 **Vertical Risk: Web-Based Malware, 2Q10**

Source: Cisco ScanSafe



What is SQL Injection?

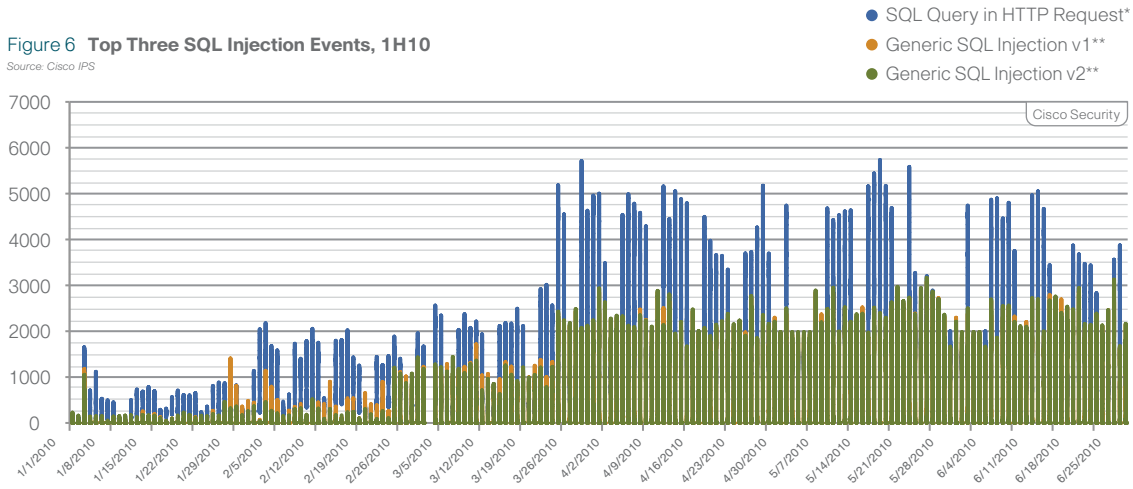
The SQL language is used to manage the data contained in relational databases and administer the SQL servers that house that data. A SQL injection attack uses malformed SQL statements in an attempt to override intended behavior and cause the SQL server to act upon the statement in an unintended fashion. SQL servers that do not properly validate input data or sanitize output data can be vulnerable to various types of SQL injection attacks. Successful attacks can lead to a range of possible compromise conditions, including the alteration of contents of a database, sensitive information disclosure, or the control of a SQL server.

SQL Injection Attacks Resume in 2Q10

The following chart reflects the top three Cisco® IPS signature events for potential SQL-injection-related attacks during the first half of 2010.

Figure 6 **Top Three SQL Injection Events, 1H10**

Source: Cisco IPS



**SQL Query in HTTP Request detects the presence of encoded words that are indicative of SQL injection attacks.*
***Generic SQL Injection v1 and Generic SQL Injection v2 detect SQL keywords in HTTP arguments*

Interestingly, a substantial increase in SQL injection events can be observed beginning in late March and early April of 2010 and extending throughout the remainder of the second quarter. This elevation in SQL injection IPS events coincides with a corresponding increase in website compromises brought on by SQL injection attacks during the same period.

The 2Q10 increase in SQL injected websites culminated with a June 2010 reappearance of Asprox. The most common cause of website compromise in mid-2008, Asprox (and all other SQL injection attacks) progressively declined throughout 2009, with Asprox completely absent in the first quarter of 2010.

Search engine results pages (SERPs) play a significant role in driving traffic to compromised websites. In 1Q10, 7.4 percent of all web-based malware encounters resulted from search engine queries. Over 90 percent of all Asprox encounters in June of 2010 were the result of SERP encounters brought on by legitimate search engine queries.

Vulnerable SQL servers were certainly not the only asset sought after by attackers in 2Q10. Observation of Cisco IPS signature event firings indicate that reconnaissance sweeps (which could be indicative of network mapping) also increased through the second quarter.

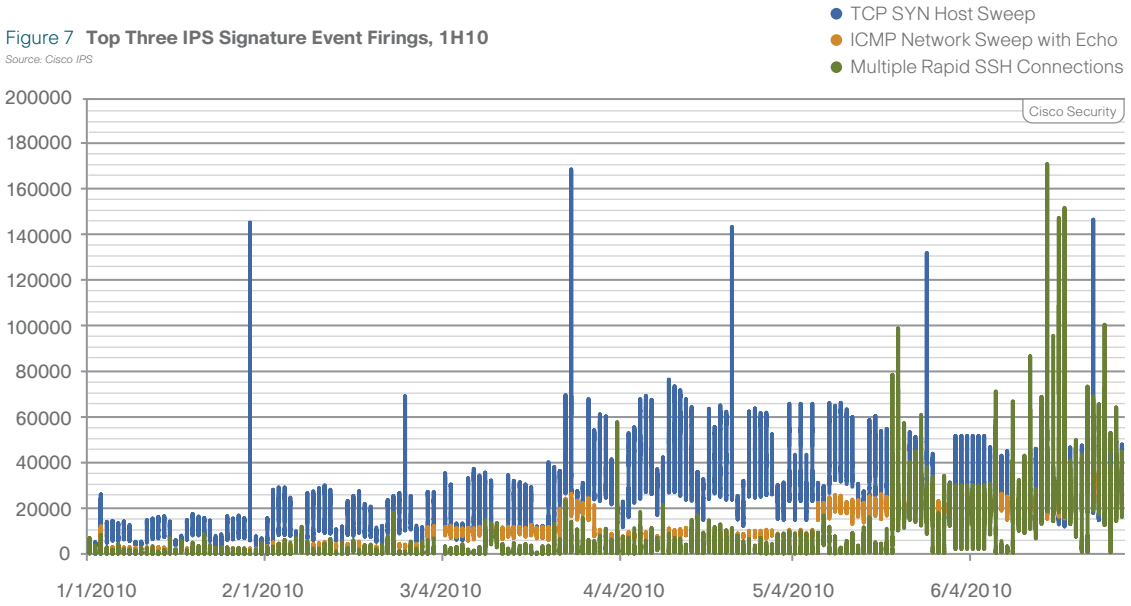
The TCP SYN Host Sweep signature fires when a series of TCP SYN packets have been sent from one single host to a number of different hosts. Typically, this behavior should not be observed from sources outside the local network but are normal behaviors for sources from within the local network (recommended filters are to exclude internal networks as sources).

Cisco Intrusion Prevention System

The Cisco Intrusion Prevention System (IPS) provides protection against over 30,000 known threats with Cisco Global Correlation to dynamically recognize, evaluate, and stop emerging Internet dangers. Global Correlation combines the inspection capability of new and existing signatures with intelligence from the Cisco SensorBase Network. Network participation and reputation are the two core components of Global Correlation. Network participation enables IPS devices to send data such as signature IDs, attacker ports and addresses, reputation scores, and risk ratings to Cisco SensorBase. Reputation provides an IPS with a probability that a given IP address is malicious. IPS devices interact with the Cisco SensorBase Network to send network participation data and receive reputation data.

Figure 7 **Top Three IPS Signature Event Firings, 1H10**

Source: Cisco IPS



ICMP Network Sweep with Echo is a medium-severity signature that triggers when IP datagrams are received directed at multiple hosts on the network with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 8 (Echo Request). Some network management tools provide network mapping capabilities which may be at least partially accomplished via a ping sweep of the network address space, resulting in a benign trigger.

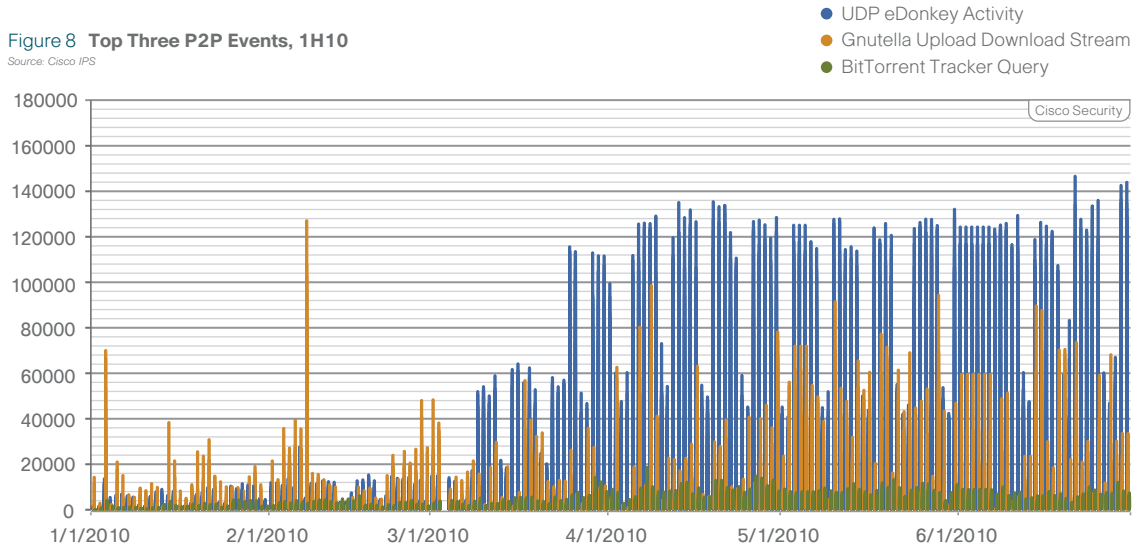
Multiple Rapid SSH Connections fire when there are rapid SSH connection from the same source to the same destination. Legitimate automated process using SSH can result in a benign trigger. The recommended action is to filter systems invoking automated SSH connections as sources for this alarm.

Wormable Risks

Increases in P2P activity observed from the end of the first quarter and persisting through the second quarter correlate with an overall increase in the number (and severity) of malware that uses P2P networks as a means of propagation.

Figure 8 **Top Three P2P Events, 1H10**

Source: Cisco IPS



By dropping malware to known P2P file shares, attackers can make any threat 'wormable' and thus enable rapid propagation. Recent variants of the Palevo family of malware include P2P infection along with Instant Messaging (IM) and autorun spread. Worm.Win32.VBNA.b, a top ten threat during 2Q10, combines autorun spread with a file-infecting virus in order to effect penetration within an enterprise.

The continued high prevalence of autorun worms in general indicates that such methods are popular with attackers—and for good reason. P2P enables wide global seeding of the malware, an ideal method for installing initial droppers or more general purposed malware. Conversely, autorun worms provide an effective means to propagate more reconnaissance-focused malware within a particular enterprise.

In June of 2010, security researchers at Belarus anti-virus firm VirusBlokAda (VBA) discovered rootkit-enabled malware that was exploiting a zero-day Windows Shell vulnerability (Microsoft Security Advisory 2286198) which enables malformed .LNK files to execute specified files automatically. The malware employing that exploit was part of a targeted attack believed to have been designed to steal SCADA design documents.

Whether via autorun or malformed .LNK files, this method of making a threat wormable can enable attackers to gain access to systems that might not otherwise be connected to the Internet or even to the wider network. Understanding normal behavior for certain types of traffic (for example, by monitoring P2P IPS events) can help identify traffic changes that could point to potential malware activity.

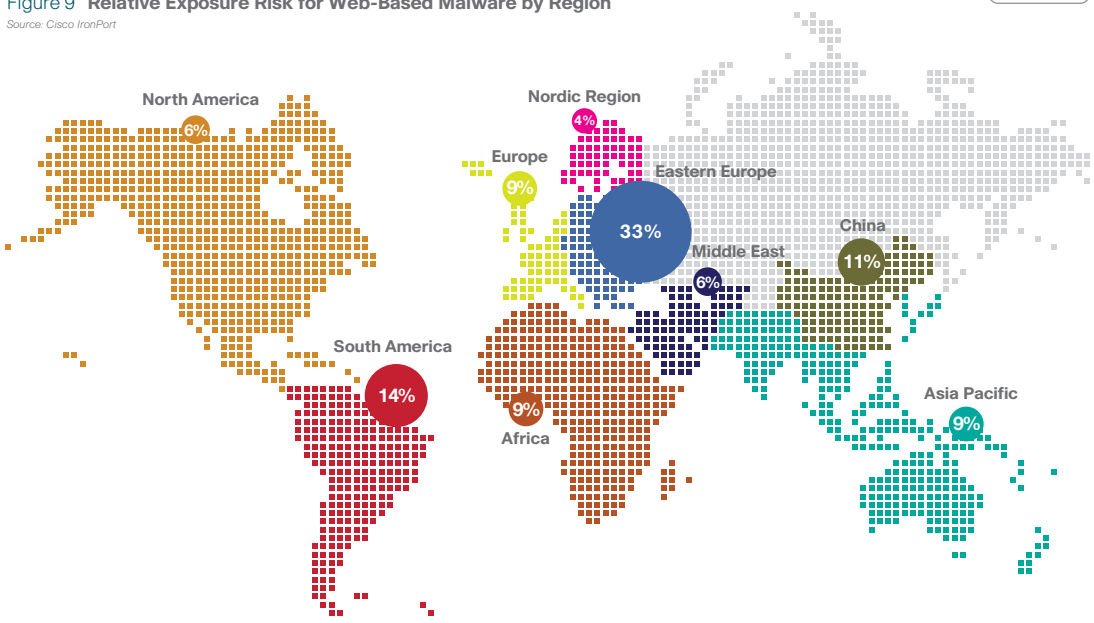
Geographic Distribution of Risk

Cisco IronPort SenderBase aggregates information from over 100,000 distinct sources across the globe. Regional risk assessment is based on a uniform sampling of data derived from participating/reporting appliances located in 78 countries. A risk rating is derived by first calculating the rate of malicious web traffic compared to legitimate traffic, based on the point of origination of the requesting appliance. That result is then compared to the results for other locales to derive the final relative exposure risk for a particular country or region.

Figure 9 **Relative Exposure Risk for Web-Based Malware by Region**

Source: Cisco IronPort

Cisco Security



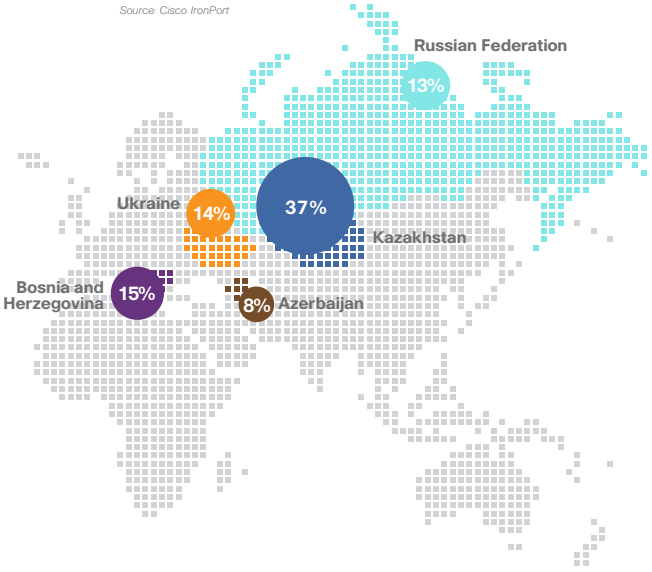
Results of the sampling indicate the regions which were most at risk for encountering web-based malware during 2Q10 were Eastern Europe (33 percent), South America (14 percent), and China (11 percent). The Nordic Region experienced the lowest level of risk, at 4 percent compared to other geographical areas.

However, these results were somewhat influenced by specific countries within a particular region that exhibited an abnormally higher or lower risk compared to other countries in that same region.

An example of this is Kazakhstan, which exhibited a 37 percent relative exposure rate among Eastern European countries, 2.5 times that of the second highest country in the region.

Figure 10 **Top Five Relative Exposure Risk for Web-Based Malware, Eastern Europe 2Q10**

Source: Cisco IronPort



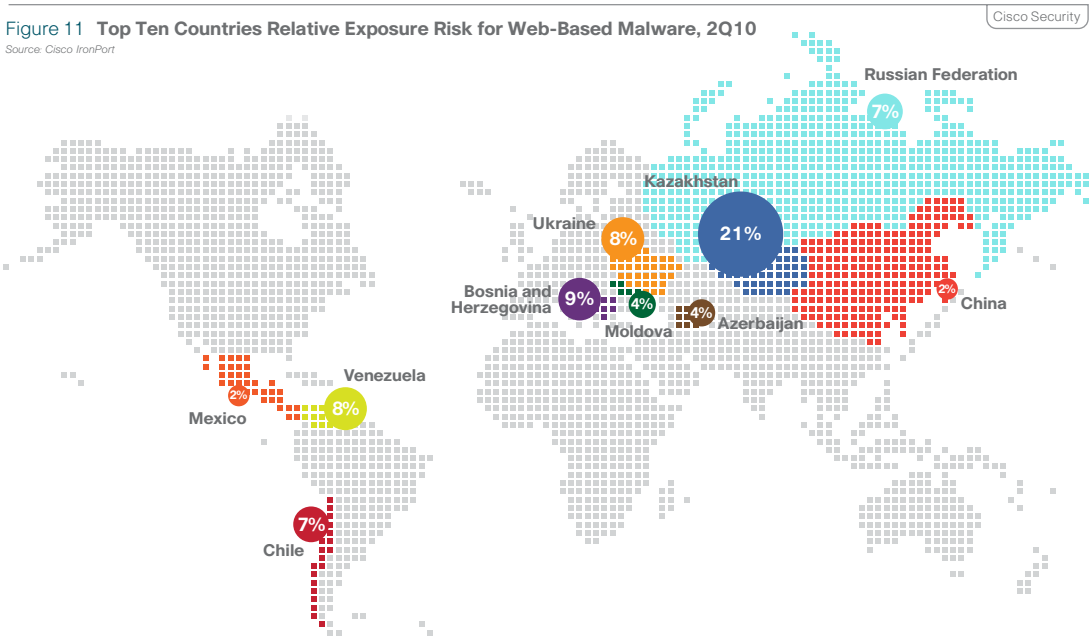
South America was largely dominated by two countries, Venezuela (41 percent) and Chile (35 percent) followed by Mexico at 10 percent.

Among countries in Europe, the spread was less dramatic with the UK at 29 percent, Spain second highest at 19 percent and France third at 11 percent.

When viewed at an individual country level, the regional bias remains evident, as seen in Figure 11.

Figure 11 **Top Ten Countries Relative Exposure Risk for Web-Based Malware, 2Q10**

Source: Cisco IronPort



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