Cisco 3Q10
Global Threat Report

Contributors:

Gregg Conklin
John Klein
Mary Landesman
Shiva Persaud
Tom Schoellhammer
Chad Skipper
Henry Stern

cisco

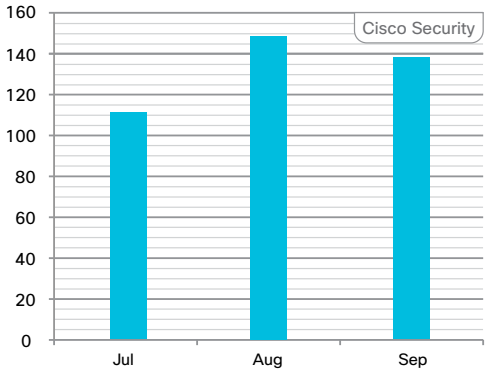
Key Highlights

- 79% of clicks on “Here You Have” email occurred within the first three hours of the worm’s spread.
- Approximately 10% of Web malware was encountered via search engine traffic and/or services.
- During 3Q10, 7% of all Web malware encounters resulted from Google referrers, followed by Yahoo at 2%, Bing/MSN at 1% and Sina at 0.1%.
- Exploits targeted Sun Java increased from 5% of all Web malware encounters in July 2010 to 7% in September 2010.
- Exploits targeting Adobe Reader and Acrobat declined over the quarter, from 3% of all Web malware blocks in July 2010 to 1% in September 2010.
- 38% of those impacted with Stuxnet were located in the UK, 25% in Hong Kong, and 13% each in Brunei, the Netherlands, and Australia.
- At 5%, the Windows Print Spooler vulnerability exploited by Stuxnet was the 5th most prevalent event handled by Cisco Remote Operations Services (ROS) in 3Q10.
- The Rustock Botnet was the highest occurring ROS event in 3Q10, at 21% of events handled during the report period.
- Peak Rustock activity occurred in late August 2010, declining in September 2010.
- Among the top ten spam sending countries, volume of spam sent also dropped in September 2010 for 8 of the top ten countries. However, spam sent from Russia and the Ukraine increased in September 2010.
- Volume of “Here You Have” email reached a peak of 10% of all spam during the worm’s initial outbreak.
- Volume of spoofed LinkedIn email delivering the Zeus Trojan reached a peak of 31.26% of all spam during a later stage of its outbreak.

Encounter Rates

Enterprise users experienced an average of 133 Web malware encounters per month in 3Q10 (see Figure 1). The number of unique Web malware hosts was highest in August, at 15,842. Unique Web malware URLs were also highest in August, at 39,001.

Figure 1 **Average Web Encounters per Enterprise, 3Q10**
Source: Cisco ScanSafe



Collectively, there were a total of 36,154 unique Web malware hosts resulting in 102,058 unique Web malware URLs in the third quarter (see Figures 2 and 3).

Approximately 10% of Web malware was encountered via search engine traffic and/or services. During 3Q10, 7% of all Web malware encounters resulted from Google referrers, followed by Yahoo at 2%, Bing/MSN at 1% and Sina at 0.1%.

Traffic resulting from the September "Here You Have" email worm was 0.3% of all Web malware encountered in September 2010. 8% of Cisco ScanSafe customers clicked through on the link contained in the worm's email. 79% of the click-through attempts occurred in the first 3 hours of the worm's spread. Cisco ScanSafe's Outbreak Intelligence™ detected and blocked all attempts.

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.

Figure 2 **Unique Web Malware Hosts, Jan-Sep 2010**
Source: Cisco ScanSafe

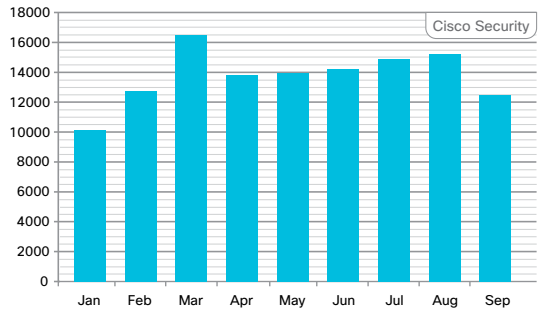
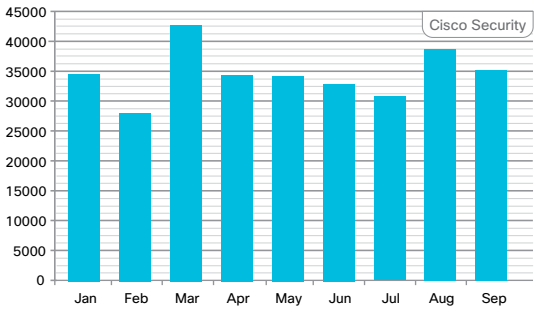


Figure 3 **Unique Web Malware URLs, Jan-Sep 2010**
Source: Cisco ScanSafe



On average, 65% of all Web malware encounters are blocked prior to exploit code or involve encounters which do not include exploit code. Of exploits that are encountered, those targeting Sun Java, Adobe Reader/Acrobat, and Adobe Flash were the three most commonly rendered during the third quarter of 2010.

Sun Java exploits increased throughout the quarter, from 5% of all Web malware blocks in July 2010 to 7% in September 2010. Conversely, PDF exploits targeting Adobe Reader and Acrobat declined over the quarter, from 3% of all Web malware blocks in July 2010 to 1% in September 2010. The third most common exploit rendered via the Web were exploits targeting vulnerabilities in Adobe Flash player, which averaged 0.4% of all Web malware encounters throughout the quarter.

The Vertical Risk

Companies in the Pharmaceutical & Chemical vertical were the most at risk for Web malware encounters in 3Q10, experiencing a heightened risk rating of 372%. Other higher risk verticals in 3Q10 included Energy, Oil, & Gas (209%), and Agriculture & Mining at 169%. The median rate for all verticals is reflected as 100% - anything above that is considered heightened risk, anything below 100% is below the median.

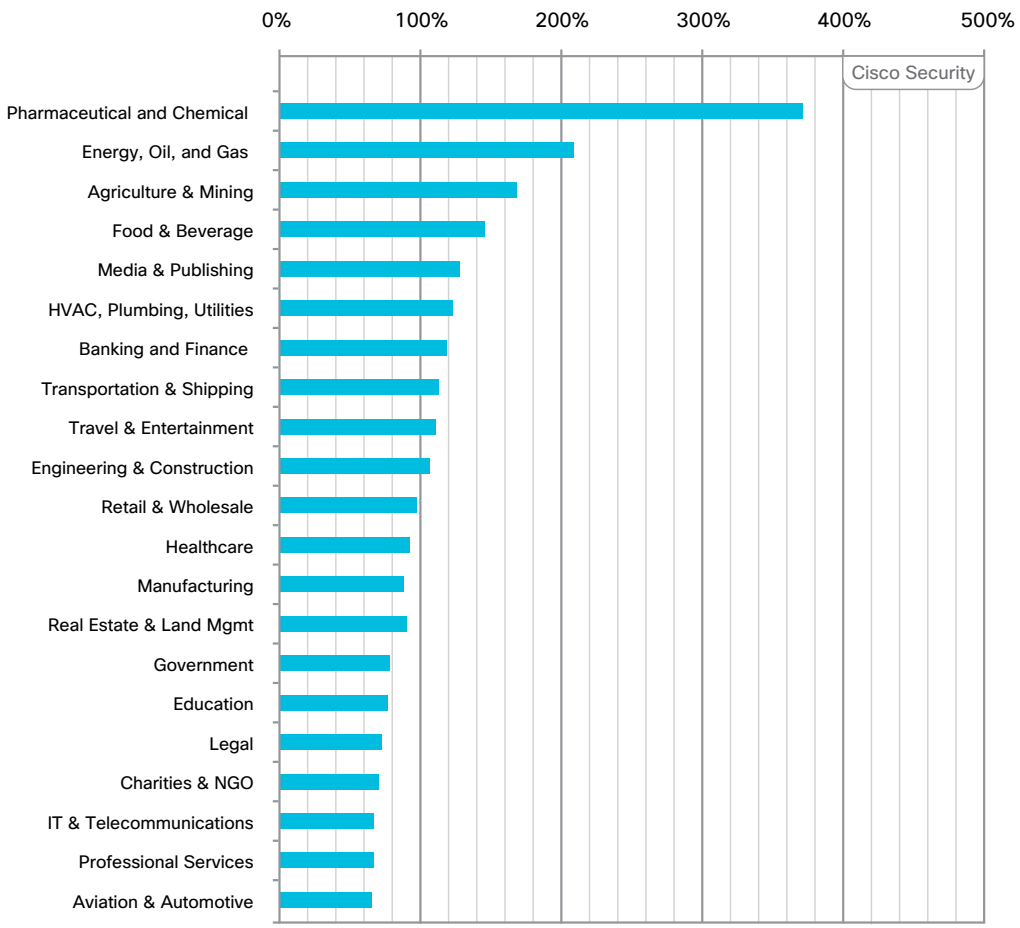
The Stuxnet Worm

The SCADA-targeting Stuxnet worm was first reported in July 2010 by Belarus antivirus vendor VirusBlokAda. That initial report was based on the analysis of a June 17th sample of the worm with the initial confirmed infection at a power plant located in Germany.

Upon successful infection, the Stuxnet worm ascertains whether an Internet connection is available and, if so, makes specially formed outbound GET requests to mypremierfutbol.com and todaysfutbol.com.

An analysis of Cisco ScanSafe Web traffic processed in the third quarter reveals that of those making the outbound request, 50% were from the Energy & Oil sector and 50% from the Pharmaceutical & Chemical industry. 38% of those impacted were in the UK, 25% in Hong Kong, and 13% each in Brunei, the Netherlands, and Australia.

Figure 4 Vertical Risk: Web Based Malware, 3Q10
Source: Cisco ScanSafe



Stuxnet and CVE-2010-2729

The vulnerability described in CVE-2010-2729 exists due to an error in the Windows print spooler service. The service fails to properly validate remote procedure call (RPC) requests and improperly determines user permissions. As a result, the service may allow an unauthorized user to print to an arbitrary file location. A Microsoft update to address this vulnerability was released in September 2010 (MS10-061).

The first known in-the-wild exploit of the vulnerability was by the Stuxnet worm, initially discovered in June 2010. During the 3Q10 report period, this vulnerability was the 5th most frequently encountered event handled by Cisco Remote Operations Services (ROS), comprising 5.08% of events handled by Cisco ROS during the third quarter. The following chart illustrates the top ten events handled by Cisco Remote Operations Security in 3Q10.

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.

The Rustock Botnet

As seen in Figure 5 above, the Rustock Botnet was the highest occurring ROS event in 3Q10, at 21% of events handled during the report period. Analysis of Cisco IPS data reveals that peak Rustock activity occurred in late August 2010, as seen in Figure 6.

Figure 5 ROS Events, 3Q10

Source: Cisco ScanSafe

Sig ID	Signature	Events
17363/3	Rustock Botnet	21.11%
5930/5	Generic SQL Injection v1	18.83%
5930/13	Generic SQL Injection v2	18.03%
13003/1	AD - External TCP Scanner	15.61%
29459/0	Microsoft Windows Print Spooler Design Flaw Vulnerability	5.08%
1203/0	IP Fragment Overwrite - Data is Overwritten	3.40%
5639/0	Web View Script Injection Vulnerability	2.60%
4055/2	B02K-UDP	1.70%
1300/0	TCP Segment Overwrite	1.66%
5081/0	WWW WinNT cmd.exe Access	1.17%

Cisco Security

Figure 6 Rustock Activity, 3Q10

Source: Cisco IPS

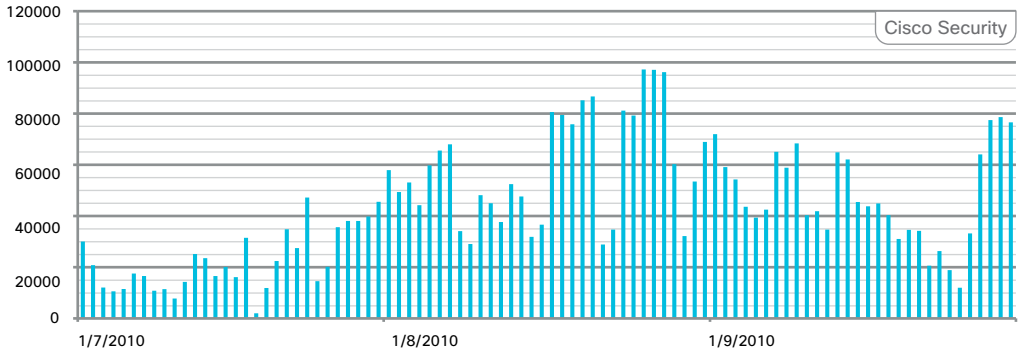
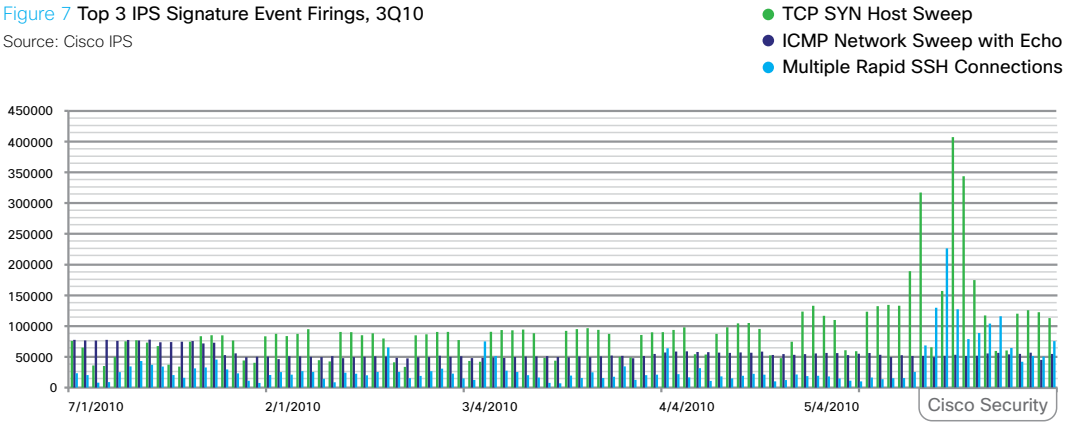


Figure 7 Top 3 IPS Signature Event Firings, 3Q10

Source: Cisco IPS



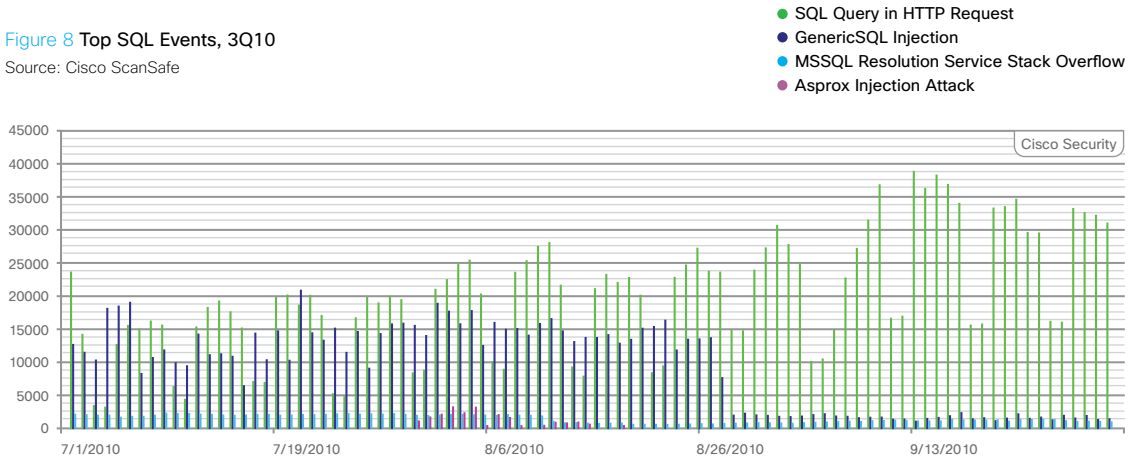
SQL Injection Attacks Continue, 3Q10

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.

The following chart reflects the top four Cisco IPS signature events for potential SQL injection related attacks during the third quarter of 2010. Asprox SQL injection attacks made a brief reappearance between July 31 and August 18, 2010.

Figure 8 Top SQL Events, 3Q10
Source: Cisco ScanSafe



SQL Query in HTTP Request detects the presence of encoded words that may be indicative of SQL injection attacks. The Generic SQL Injection event signature detects the presence of SQL keywords in HTTP arguments. MSSQL Resolution Service Stack Overflow is detection for SQL/Slammer activity.

In terms of port activity, 54% of Cisco Remote Operations Services (ROS) events handled occurred on port 80, followed by port 445 at 18% and port 25 at 15%.

Global Spam Trends

Analysis of Cisco IronPort data indicates that spam volumes were highest in August 2010 compared to the remainder of the quarter. Spam volume fell from 326 billion spam per day in August 2010 to 257 billion per day in September 2010.

The Rustock botnet is believed to be one of the largest purveyors of spam, with the largest number of Rustock bots reportedly located in the U.S. Rustock has been most predominantly affiliated with sending pharmaceutical and counterfeit watch spam, often in the form of a breaking news alert (a tactic first popularized by the Storm botnet).

Figure 9 Events by Port
Source: Cisco ROS

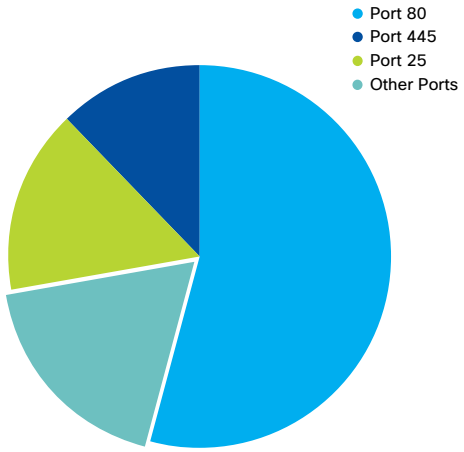
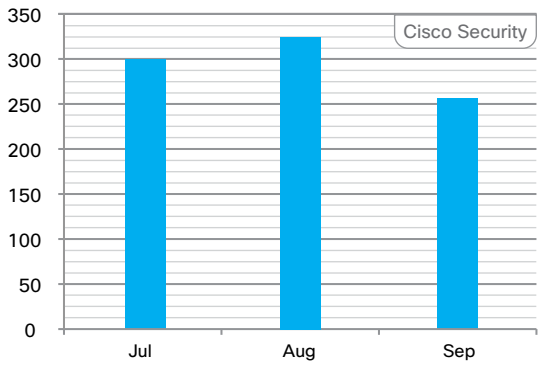


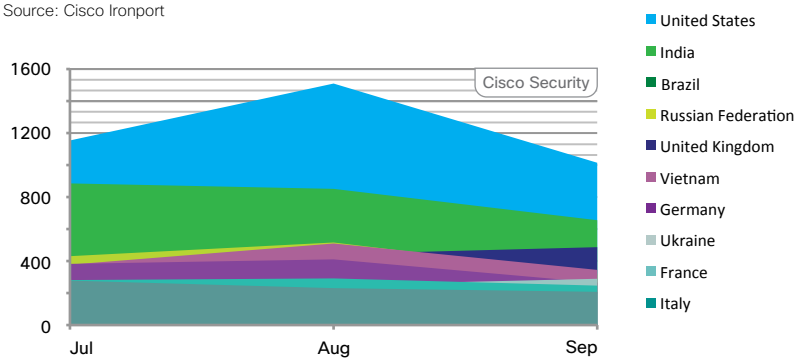
Figure 10 Global Spam Volume (Bn/Day), 3Q10
Source: Cisco Ironport



As previously observed in Figure 6, peak Rustock activity was in August 2010 followed by a decline in September 2010, mimicking the pattern observed with spam volumes during the same period.

Among the top ten spam sending countries, volume of spam sent similarly dropped for eight of the ten. However, spam sent from Russia and the Ukraine increased in September 2010. Figure 11 illustrates spam volumes originating from the top ten spam senders in 3Q10.

Figure 11 **Top Spam Senders by Country, (Bn/Mo), 3Q10**
Source: Cisco Ironport

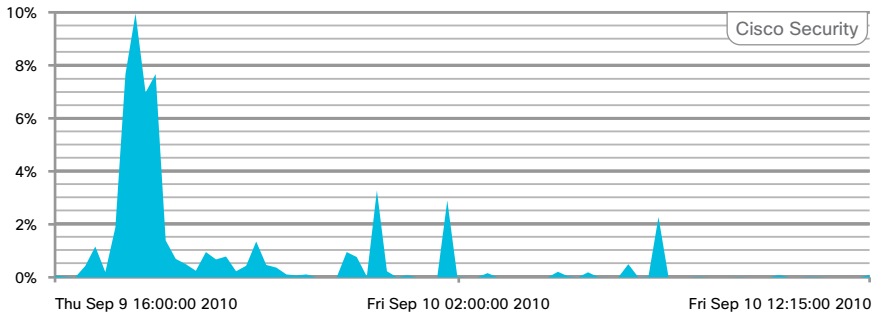


"Here You Have" Email Worm

On September 9, an email bearing the subject line "Here you have" began arriving in users' inboxes. The email included a link disguised as a PDF which actually pointed to a a copy of the worm. As users clicked through to the link and became infected, the wom sent an identical message to all contacts in the newly infected user's address book.

Fortunately, the malware domain hosting the worm's binary was taken offline within 3 hours of the worm's spread. This neutered the worm's ability to propagate further, though not before significant volumes were observed in email as seen in Figure 12.

Figure 12 "Here You Have" **Email as a Percentage of All Spam**
Source: Cisco Ironport



Fake LinkedIn Email

Also occuring in September, a spoofed LinkeIn email masqueraded as a standard LinkedIn alert (see Figure 14).

Recipients that clicked the links in the email were directed to a wepage which responded with "PLEASE WAITING.... 4 SECONDS" after which they were redirected to Google.com. During the 4 seconds, exploit code was rendered on the victim's PC in an attempt to silently install a varient of the Zeus data theft trojan.

Zeus injects itself as a process in the user's web browser and launches a man-in-the-browser attack to capture personal information such as online banking credentials. Infected systems are also joined to the Zeus botnet, after which the infected computers may be used to launch additional attacks on others.

During the course of the largest LinkedIn spoofing in mid-September, the maliicous LinkedIn email comprised 31.26% of all spam for that period (Figure 15).

Figure 13

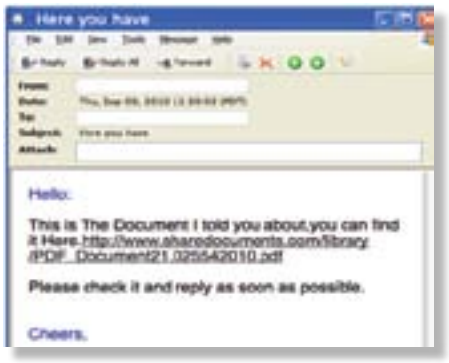
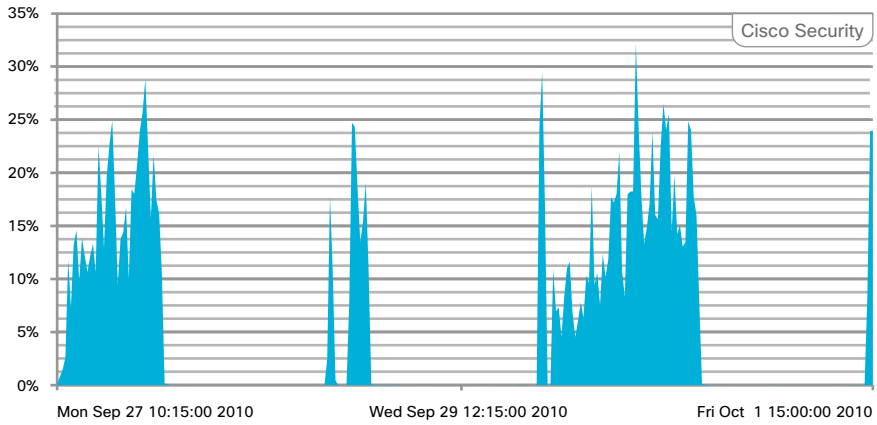


Figure 14

Figure 15 Fake LinkedIn Email as a Percentage of All Spam

Source: Cisco Ironport



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

