

Cisco 2009 Midyear Security Report

[View the Cisco Midyear Security Report video](#)



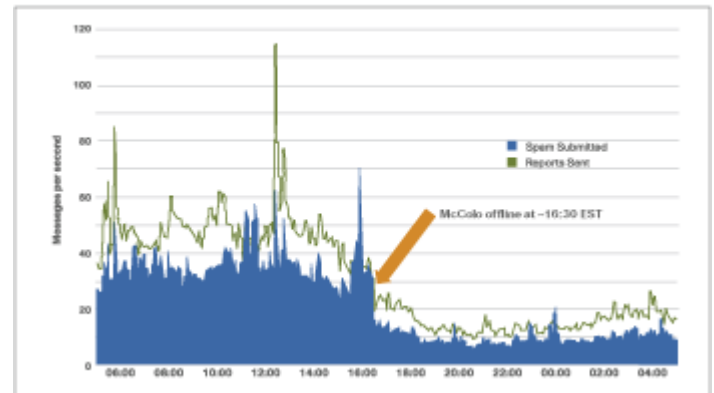
An Update on Global Security Threats and Trends

The *Cisco 2009 Midyear Security Report* presents an overview of Cisco's security intelligence, highlighting threat information and trends from the first half of 2009. The report also includes recommendations from Cisco security experts and predictions of how identified trends will evolve.

[Download the full Report Now](#)

As predicted the Cisco 2008 Annual Security Report, attacks are only becoming more sophisticated and targeted as we move through 2009. Even as the global economy struggles to recover, online crime remains a healthy moneymaker for its participants. Criminals are embracing technical innovation, and collaborating with other enterprises to develop new strategies for generating income. Botnet owners, for example, are working together to build partnerships and maximize profits.

Spam Volume Decline Due to McColo Shutdown



"We see many signs that criminals are mimicking the practices embraced by successful, legitimate businesses to reap revenue and grow their enterprises," said Tom Gillis, Vice President and General Manager of Cisco Security Products. "It seems the best practices espoused by Fortune magazine and Harvard Business School have found their way into the online underworld."

As online criminals adapt and refine their techniques for generating revenue, security professionals and individual computer users must become even more sophisticated in their own approaches to combating security threats. There are encouraging signs that collaboration among the "good guys" is thwarting attacks more quickly, and helping to bring criminals to justice.

Meanwhile, in the United States, the Obama administration has made strengthening the nation's cybersecurity a high priority, and looks to leverage technology innovation and partner with the private sector. Other countries, including the United Kingdom and Finland, are also stepping up their efforts to enhance cybersecurity and prevent cybercrime.

Additional Highlights

- Criminals are exploiting supposed "old-school" vulnerabilities because they believe security experts and individual computer users are paying minimal attention to these types of threats.
- Compromising legitimate websites for the purpose of propagating malware remains a highly effective technique for criminals.
- Web 2.0 applications, prized for their ease of use and flexibility, have become lures for criminals.
- The good buzz about cloud computing may be overshadowed by the possible security risks, and businesses do not have a clear plan for protecting data in the cloud.
- Criminals are targeting people who use online banking with well-designed, localized text message scams—and they're leaving virtually no trail.

Key Recommendations

Security must move at the speed of crime—Businesses and individual computer users must become more agile in deploying countermeasures and responding to attacks.

User education and security awareness training are critical—Employees should play a vital role in safeguarding their own online identity and understanding the risks that can accompany technology use.

Keep an eye on "old problems" while being vigilant about new risks—Unpatched or forgotten machines can provide attackers with an "agent behind enemy lines" for inside-the-firewall attacks.

Never underestimate the insider threat, particularly in an uncertain economy—Insiders know how to exploit an organization's weaknesses and security policies to steal data or money, or disrupt operations.

While it's true that cybercrime is becoming more pervasive, and the online criminal economy is maturing, there are bright spots. More cybercriminals are being identified and prosecuted – and are going to jail. In addition, the number of vulnerabilities and discrete threats has been off to a slower start this year compared to 2008, according to research by Cisco—a sign the security community is succeeding in making it more difficult for attacks to take root and grow.

2009 Threats and Vulnerabilities:
25 Percent Decrease From 2008 Activity Levels

Month	New Alerts	Updated Alerts	2009 Total	2008 Total
January	148	392	540	630
February	227	249	476	695
March	222	335	557	659
April	164	206	370	639
May	218	175	393	528
Totals	979	1357	2336	3151