



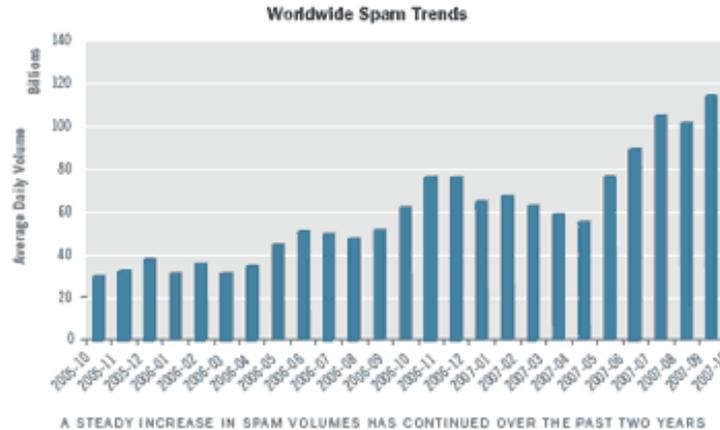
Internet Security Trends
for 2008

2008 INTERNET SECURITY TRENDS

TRENDS OVERVIEW

The overall trends in spam and malware can be characterized by a larger number of more targeted, stealthy and sophisticated attacks. Specific observations include:

- **Spam volume increased 100 percent, to more than 120 billion spam messages daily worldwide.**



- **Spam has become more dangerous.** Earlier versions of spam attacks were primarily selling some type of product. In 2007, more than 83 percent of spam contained a URL to a rogue Web server that was frequently serving malware. In accordance with a trend towards the blending of different malware techniques, URL-



[IronPort. Award-Winning Security.](#)

IronPort 2008 Trends Report
[Download now](#)

IronPort PXE Encryption
[How It Works](#)

Web Security Report
September 2007 issue
now available. [More](#)

Sign-Up

based viruses increased 200 percent.

- **The "Self Defending Bot Network" was introduced.** The Storm Trojan is perhaps one of the most sophisticated botnets ever observed. It uses a peer-to-peer (P2P) control scheme to avoid a single control node that would give it away. When researchers or security vendors probe Storm-related Web servers, the Storm Trojan will launch a DDoS attack and relocate the Web server. The quality of the websites delivered by Storm, and the remarkable technical sophistication of the underlying peer-to-peer network, reflect that these threats are being developed by professional engineers.
- **Viruses no longer make headlines**, because virus writers have evolved from the previous mass distribution attacks such as Netsky and Bagel. In 2007, viruses were much more polymorphic and typically associated with the proliferation of very sophisticated botnets such as Feeps and Storm.

TOP VIRUS OUTBREAKS		
2005	2006	2007
Mytob	Stration	Storm
Bagle	Bagle	Feeps
Sober	Mytob	Clagger

[Download the 2008 Trends Report](#)

REPORT FINDINGS

Spam Still Pays

2007 was the year of spam attachments. Spammers conducted trials of more than 20 different file attachment types to determine which had the best success rates. Rapid onset spam attacks became commonplace, with outbreaks spiking in volume very quickly and anti-

For Real-Time Virus

Threat Level Updates.

[More](#)

Information For:

- + Government Agencies
- + Education
- + ISPs
- + Resellers
- + Healthcare
- + Financial Services

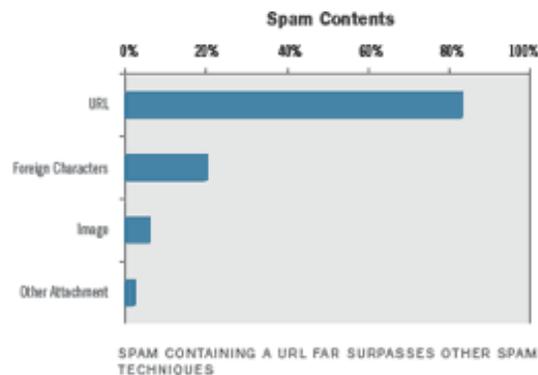
Information About:

- + Email Encryption
- + IronPort Anti-Spam
- + Virus Outbreak Filters
- + Web Security
- Appliances
- + How to Buy

spam companies scrambling to adapt. This left little reaction time, and many anti-spam

customers found themselves reevaluating anti-spam products that could not adapt.

Many of the most malicious attacks start as a seemingly innocuous spam message with nothing more than a few words of text and a single URL. These messages often slip past traditional spam engines that are looking for

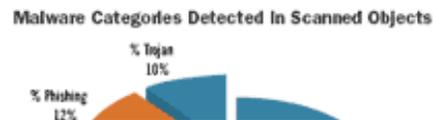


keywords, or for graphics touting the latest stock spam. When they land in the recipient's inbox they have made it to the most sensitive part of the corporate network. All it takes is one errant click of the mouse and the payload is downloaded - providing full access to the user's computer, and possibly the internal network.

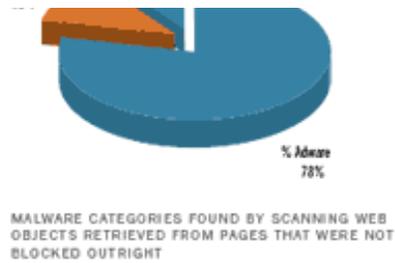
Malware Platforms

Storm and MPack dominated much of the Internet security news in 2007, but not just because of their size and scope. They both introduced new, more sophisticated techniques that demonstrate the refinement of malicious software. Malware creators are spending more time and resources developing an actual platform that is designed to last and be reused. Delivery methods are also changing, moving toward blended attacks that combine both email and Web services.

Attacks are now originating from directly inside the "protected" corporate network. Many administrators



believe they have secured their infrastructures and that spam is nothing more than an irritant. The truth: spam is being used as a gateway, designed to lure users to dangerous sites. To respond,



companies must deploy the most advanced email security systems to stop inbound threats, enforce strong classification and scanning of all user-initiated Web traffic and monitor closely for possible internal malware infections. Also being seen is a higher frequency of attacks, timed to coincide with popular events and major news stories in an attempt to both make the message seem more legitimate. These attacks are designed to maximize the spread of malicious content by piggy-backing on strong public interest in sports, political activities, or natural disasters.

"You have to look at the trends of the next decade and plan for it. We all understand the trend - security incidents are getting worse. You can't predict when and where things will happen, so you'll have to understand the how."

John Chambers

Chairman and Chief Executive Officer, Cisco Systems

Corporations are under increasing pressure to ensure the integrity of their sensitive information. IT security teams need to take steps to measure malicious traffic in their network and deploy a comprehensive security system that includes advanced techniques,

such as network-based threat detection and network access control.