Cisco 4Q11

Global Threat Report

Contents

Key Highlights

- Enterprise users experienced an average of 339 Web malware encounters per month in 4Q11.
- An overall average of 362 Web malware encounters per month occurred throughout 2011.
- The highest rate of encounters occurred during September and October 2011 at 698 and 697 on average per enterprise, respectively.
- An average of 20,141 unique Web malware hosts were encountered per month in 2011, compared to a monthly average of 14,217 in 2010.
- During 4Q11, 33 percent of Web malware encountered was zero-day malware not detectable by traditional signature-based methodologies at the time of encounter.
- The highest rate of zero-day malware blocks for the quarter occurred in November 2011, during which 47 percent of Web malware was blocked by Outbreak Intelligence™.
- The rate of SQL injection signature events remained fairly steady throughout 4Q11, with a slight decrease observed as the quarter progressed.
- Denial-of-service events increased slightly over the course of 4Q11.
- Global spam volumes continued to decline throughout 2011.

All contents are Copyright © 2012 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Introduction

The proper security tools can prevent infection or stop outbreaks, mitigate or reduce losses from malicious events, and even decrease legal liability. These products can also often serve as an excellent source of information about what is happening in your 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 indicate 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 associations to global non-malware-related events. Most importantly, regular review and understanding of the data can help uncover the elusive “black swan”—the types of surreptitious and malicious events that otherwise could fly below the radar.

The Cisco Global Threat Report is a compilation of data collected across four core segments of Cisco Security: ScanSafe, Intrusion Prevention System (IPS), Remote Management Services (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 4Q11 Global Threat Report include

Vicki Byrd
Gregg Conklin
Mary Landesman
Armin Pelkmann
Shiva Persaud

All contents are Copyright © 2012 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Cisco ScanSafe: Web Malware Events

Enterprise users experienced an average of 339 Web malware encounters per month in 4Q11, a 205 percent increase compared to 4Q10. An overall average of 362 Web malware encounters per month occurred throughout 2011, compared to a monthly average of 135 in 2010. The highest rate of encounters occurred during September and October 2011 at 698 and 697 on average per enterprise, respectively.

An average of 20,141 unique Web malware hosts were encountered per month in 2011, compared to a monthly average of 14,217 in 2010. Despite the marked increase in average Web malware encounters in September and October 2011, the rate of unique hosts remained steady for those months.

Figure 1 Average Web Encounters per Enterprise, 2010–2011
Source: Cisco ScanSafe

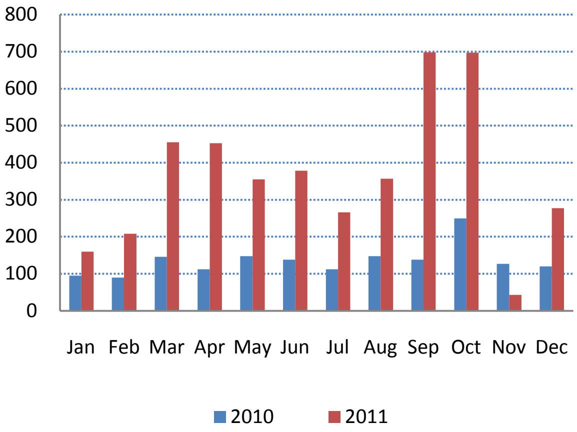


Figure 2 Unique Web Malware Hosts, 2010–2011
Source: Cisco ScanSafe

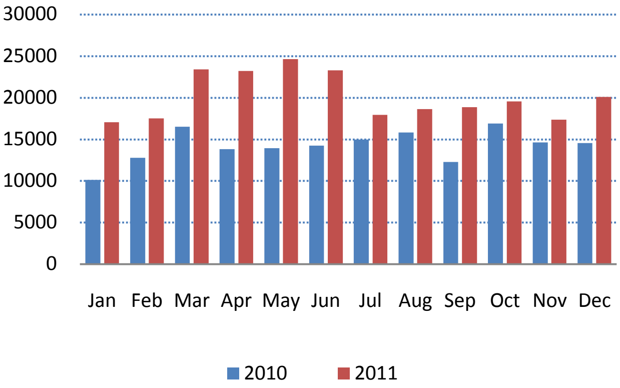
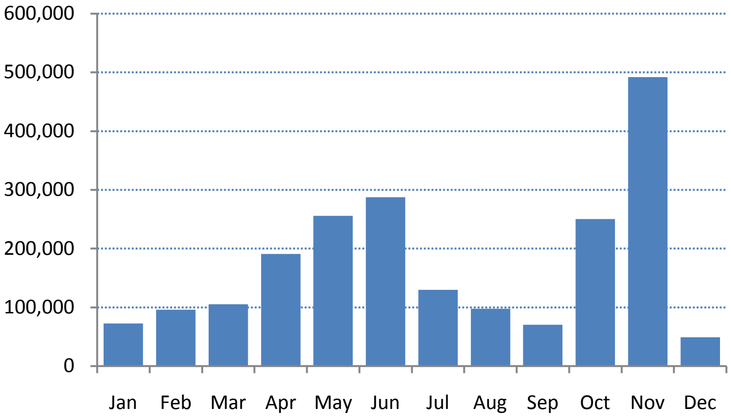


Figure 3 Unique Web Malware, 2011
Source: Cisco ScanSafe



The rate of unique Web malware (as determined by unique MD5 hash recorded) was considerably varied from month to month over the course of 2011. The highest volume of unique Web malware (491,750) occurred in November 2011. This sharp increase in November was immediately followed by an even sharper decrease in December 2011, in which only 49,239 unique Web malware were recorded for the month.

During 4Q11, 33 percent of Web malware encountered was blocked by ScanSafe Outbreak Intelligence™. These zero-day malware blocks indicate malware not detectable by traditional signature-based methodologies at the time of encounter. The highest rate of zero-day malware blocks for the quarter occurred in November 2011, during which 47 percent of Web malware was blocked by Outbreak Intelligence™.

All contents are Copyright © 2012 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

At 422 percent, companies in the Pharmaceutical & Chemical sector had the highest overall Web malware encounter risk, followed closely by Agriculture & Mining at 343 percent and companies in the Energy & Oil sector at 333 percent.

Throughout each quarter of 2011, companies in the Pharmaceutical & Chemical sector continually experienced the highest median Web malware encounter rate compared to companies in other sectors.

To determine the risk rating for each vertical, a median encounter rate for all enterprises across all sectors is calculated. The median encounter rate for enterprises in each individual sector is then calculated. These median rates are then compared to determine whether a particular sector is at heightened or lowered risk of Web malware encounters.

Figure 4 Web Malware Encounter Risk by Sector, 4Q11

Source: Cisco ScanSafe

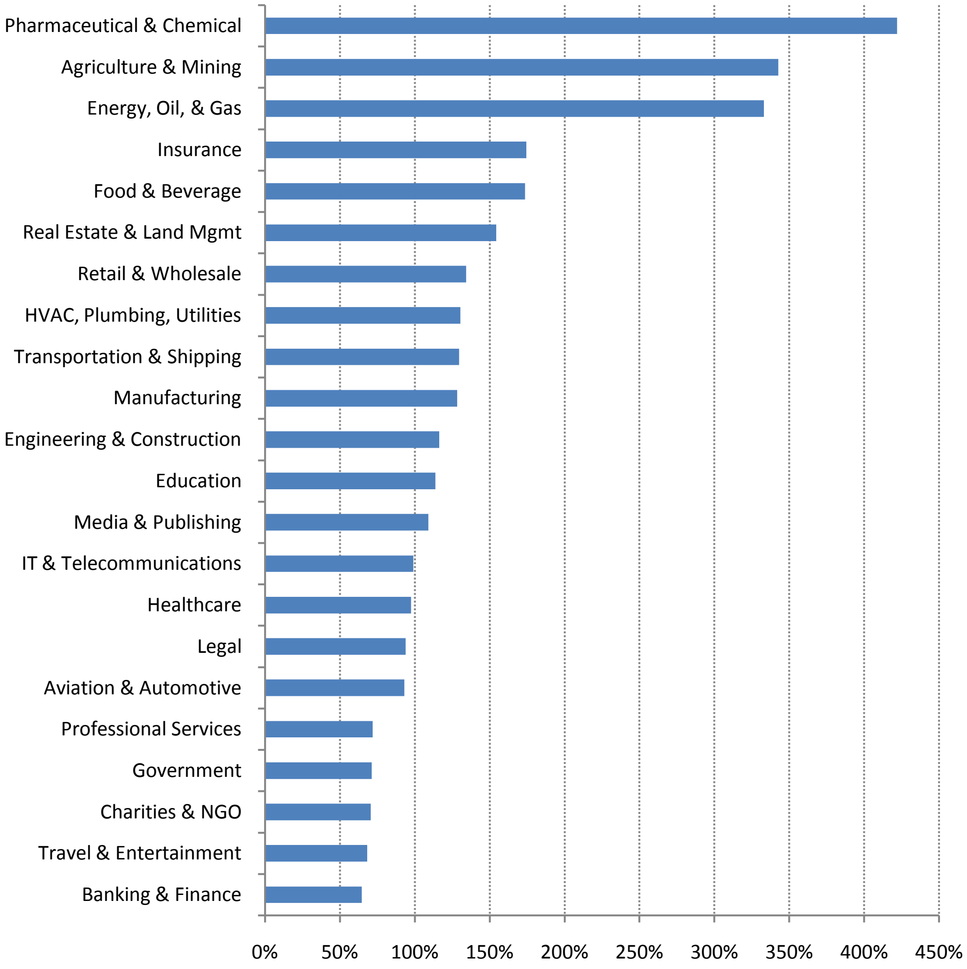
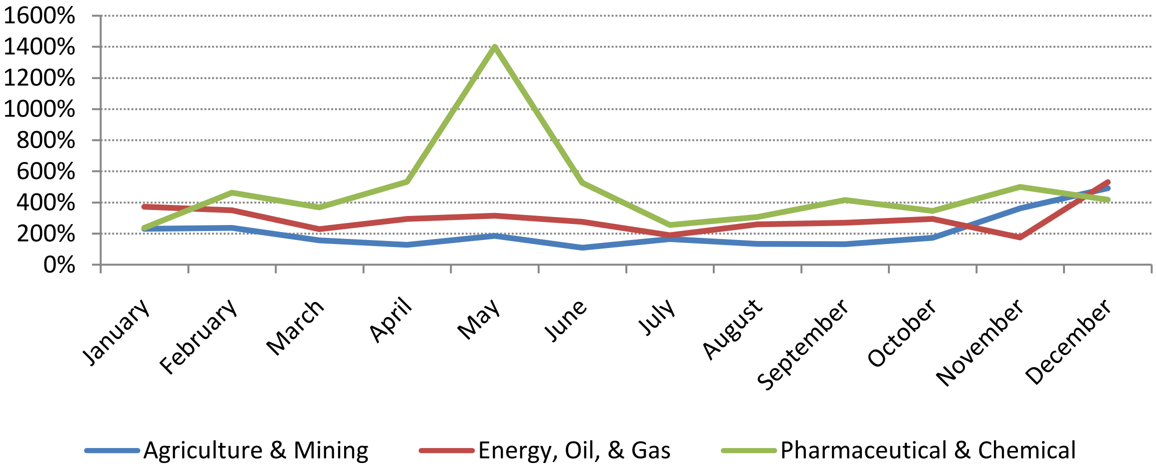


Figure 5 Top Three Highest Risk Sectors, 2011

Source: Cisco ScanSafe



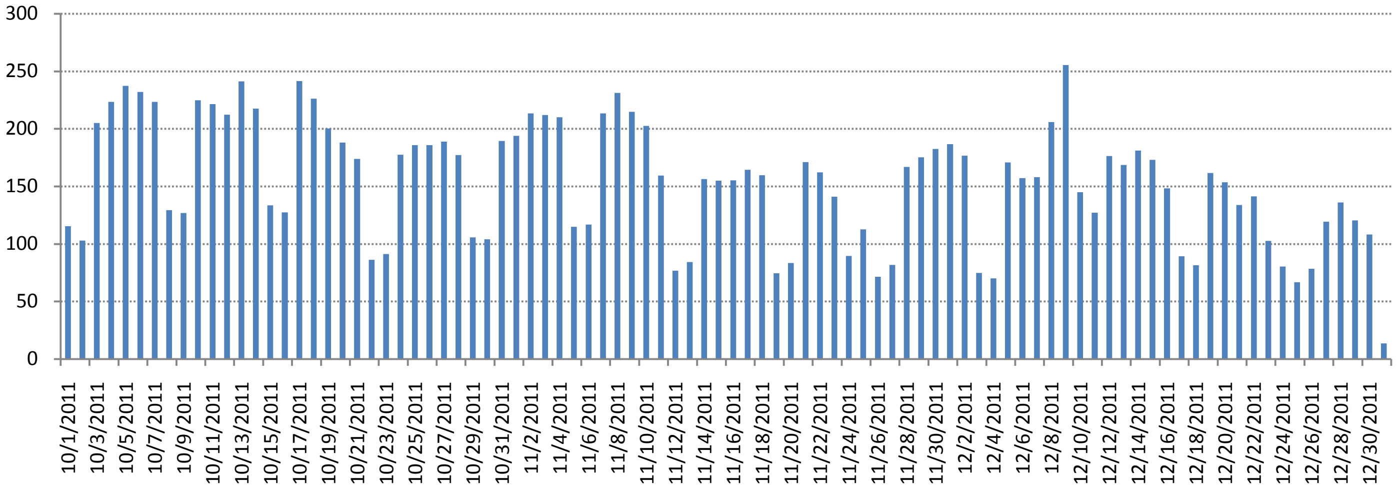
All contents are Copyright © 2012 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Cisco Intrusion Prevention System

SQL injection attempts remained at a fairly steady pace throughout 2011, with a subtle reduction observed in the fourth quarter. Figure 6 illustrates the average SQL injection signature firing events by reporting sensor during 4Q11.

Figure 6 SQLi Events by Average Sensor Volume, 4Q11

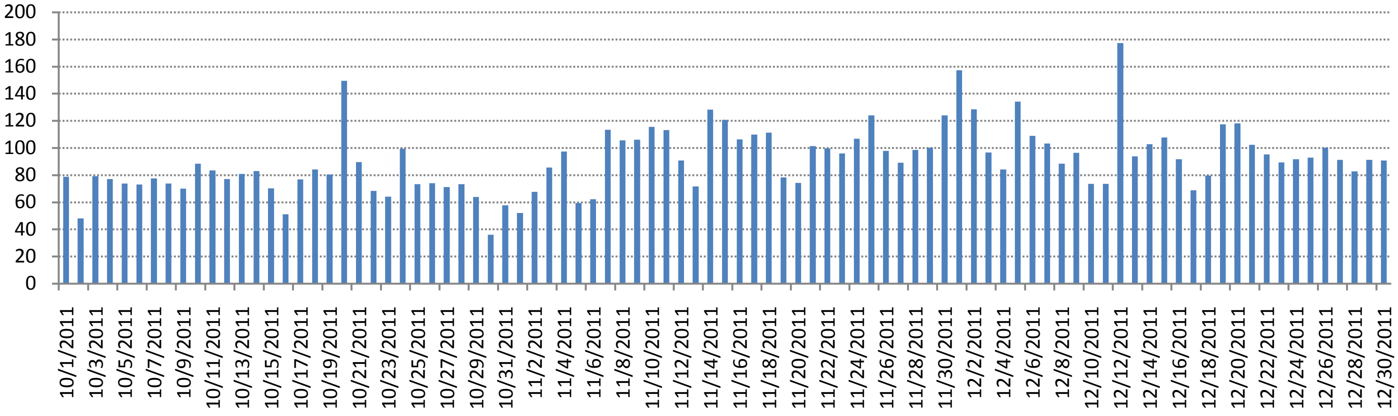
Source: Cisco IPS



Denial-of-service (DoS) attacks also had a steady presence throughout 4Q11, but with a converse slight increase occurring as the quarter progressed. While once largely prank related, DoS attacks are increasingly politically and financially motivated.

Figure 7 DoS Events by Average Sensor Volume, 4Q11

Source: Cisco IPS



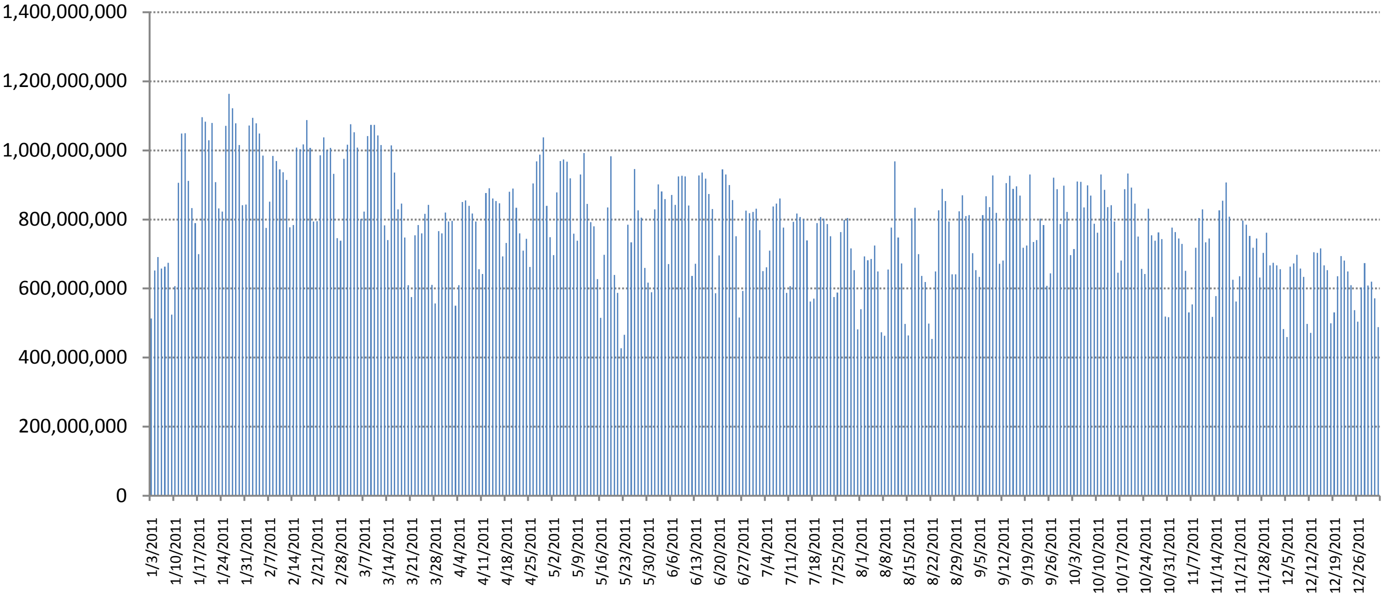
All contents are Copyright © 2012 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Cisco IronPort: Global Spam Trends

The 2011 takedown of segments of Rustock, combined with multiple spam botnet takedowns in 2010, continues to have a positive impact on overall spam volume. Figure 8 reflects global spam volume as reported through Cisco SenderBase Network participants.

Figure 8 Global Spam Volume, 2011

Source: Cisco IronPort (SBNP/ESA)



All contents are Copyright © 2012 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

About the Contributors

Cisco ScanSafe

Cisco ScanSafe provides Web security in the cloud, offering both Web request and content security.

http://www.scansafe.com

Cisco Intrusion Prevention System

The Cisco Intrusion Prevention System provides threat control by inspecting traffic as it traverses the network and providing information or taking action to prevent unwanted activity.

http://www.cisco.com/en/US/products/ps5729/Products_Sub_Category_Home.html

Cisco Remote Management Services

Cisco Remote Management Services help organizations manage, monitor, and protect their networks using industry best practices.

http://www.cisco.com/en/US/products/ps6192/serv_category_home.html

Cisco IronPort

Cisco IronPort provides e-mail and Web security, either in the cloud or through appliances.

http://www.cisco.com/web/about/ac49/ac0/ac1/ac259/ironport.html

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.**

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)