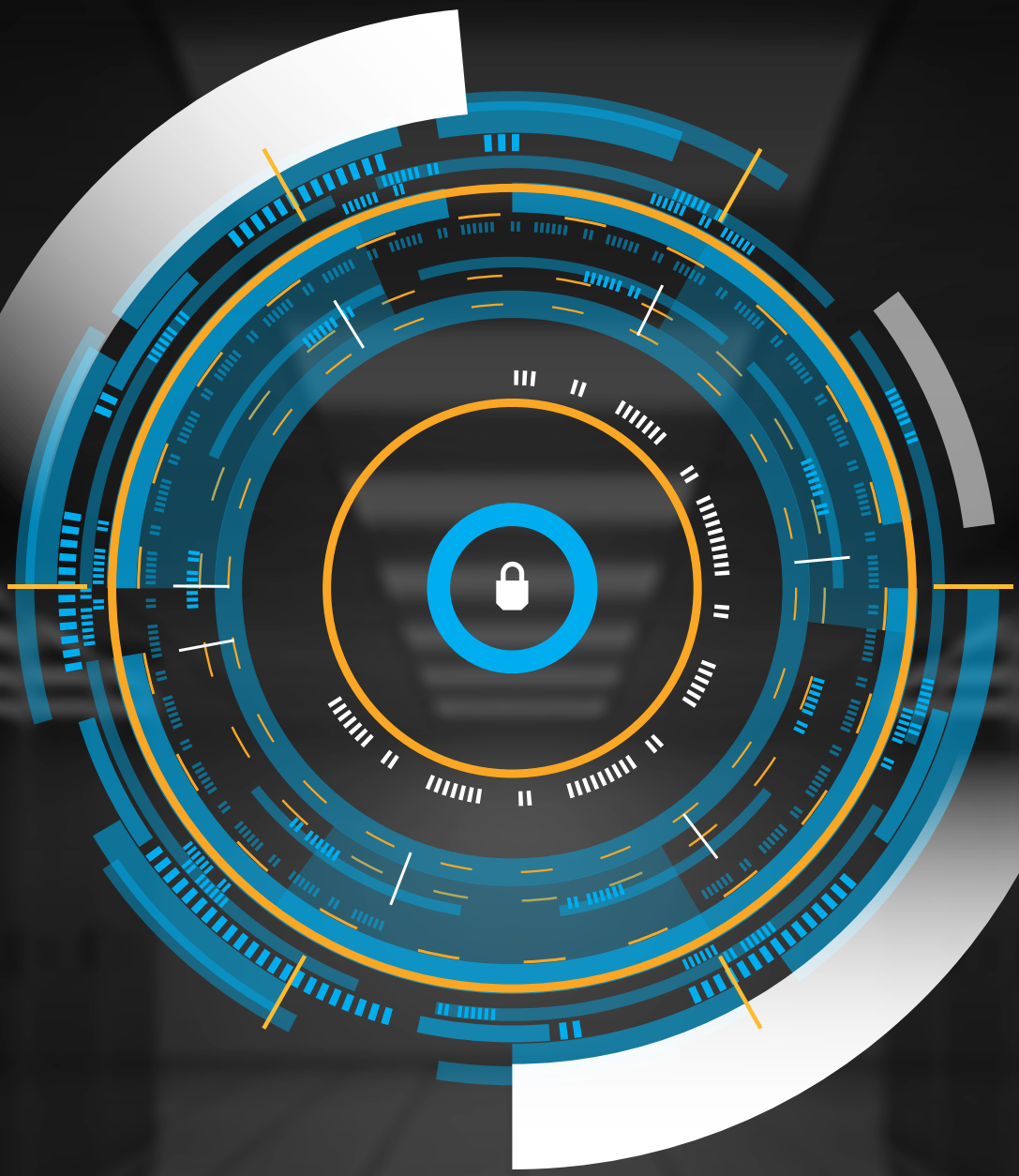


ISTR

Internet Security Threat Report | Appendices

VOLUME 21, APRIL 2016

Symantec

CONTENTS

APPENDIX A: THREAT ACTIVITY TRENDS

The following section of the Symantec Internet Security Threat Report provides an analysis of threat activity, data breaches, and web-based attacks, as well as other malicious actions that Symantec observed in 2015. The malicious actions discussed in this section also include phishing, malicious code, spam zombies, bot-infected computers, and attack origins. Attacks are defined as any malicious activity carried out over a network that has been detected by an intrusion detection system (IDS) or firewall. Definitions of the other types of malicious activities can be found in their respective sections within this report.

This section will discuss the following metrics, providing analysis and discussion of the trends indicated by the data:

- Malicious Activity by Source
- Bot Infected Computers

MALICIOUS ACTIVITY BY SOURCE

Background

Malicious activity usually affects computers connected to high-speed broadband Internet. These connections are attractive targets for attackers, because they provide larger bandwidth capacities than other connection types, faster speeds, and typically offer a more stable connection—with potential for constantly connected systems.

Symantec categorizes malicious activities as follows:

- **Malicious code.** This includes programs such as viruses, worms, and Trojans that are covertly inserted into programs. The purposes of malicious code include destroying data, running destructive or intrusive programs, stealing sensitive information, and compromising the security or integrity of a victim's computer data.
- **Spam zombies.** These are remotely controlled, compromised systems specifically designed to send out large volumes of junk or unsolicited email messages. These email messages can be used to deliver malicious code and phishing attempts.
- **Phishing hosts.** Phishing hosts are computers that provide website services in order to illegally gather sensitive user information while pretending that the attempt is from a trusted, well-known organization by presenting a website designed to mimic the site of a legitimate business.
- **Bot-infected computers.** Malicious programs have been used to compromise computers to allow an attacker to control the targeted system remotely. Typically, a remote attacker controls a large number of compromised computers over a single reliable channel in a botnet, which can then be used to launch coordinated attacks.
- **Network attack origins.** This measures the originating sources of attacks from the Internet. For example, attacks can target SQL protocols or buffer overflow vulnerabilities.
- **Web-based attack origins.** This measures attack sources that are delivered via the web or through HTTP. Typically, legitimate websites are compromised and used to attack unsuspecting visitors.

Methodology

These metrics assess the sources from which the largest amount of malicious activity originates. To determine malicious activity by source, Symantec has compiled geographical data on numerous malicious activities, namely malicious code reports, spam zombies, phishing hosts, bot-infected computers, network attack origins, and web-based attack origins. The proportion of each activity originating from each source is then determined. The mean of the percentages of each malicious activity that originates in each source is calculated. This average determines the proportion of overall malicious activity that originates from the source in question, and rankings are determined by calculating the mean average of the proportion of these malicious activities that originated in each source.

Data and Commentary

Figure A.1. Malicious Activity by Source: Overall Rankings, 2014-2015

Geography	2015 World Rank	2015 Overall Average	2014 World Rank	2014 Overall Average	Annual Change	Change in Number of Attacks Originating from Geography
China	1	23.7%	2	10.6%	+13.1%	-20.0%
United States	2	18.9%	1	20.7%	-1.8%	-64.3%
India	3	3.4%	3	4.0%	-0.6%	-51.3%
Netherlands	4	2.8%	4	3.6%	-0.8%	-41.2%
Taiwan	5	2.4%	6	2.6%	-0.2%	-53.1%
Turkey	6	2.3%	20	1.2%	+1.1%	-52.4%
United Kingdom	7	2.3%	7	2.6%	-0.3%	-61.0%
Germany	8	2.2%	5	3.3%	-1.0%	-65.2%
France	9	2.1%	14	1.9%	+0.2%	-47.4%
Brazil	10	2.0%	10	2.3%	-0.3%	-41.7%

Figure A.2. Malicious Activity by Source: Malicious Code, 2014-2015

Geography	2015 Malicious Code Rank	2015 Malicious Code %	2014 Malicious Code Rank	2014 Malicious Code %	Annual Change	Change in Number of Attacks Originating from Geography
United States	1	13.7%	1	19.8%	-6.1%	-67.4%
India	2	12.5%	2	12.2%	+0.3%	-52.1%
China	3	10.7%	3	6.5%	+4.2%	-22.9%
Netherlands	4	3.8%	6	3.3%	+0.5%	-45.5%
Indonesia	5	3.8%	7	3.2%	+0.7%	-43.0%
Australia	6	3.0%	8	3.0%	-	-52.7%
Brazil	7	2.8%	11	2.3%	+0.5%	-43.9%
Vietnam	8	2.6%	10	2.4%	+0.2%	-49.2%
United Kingdom	9	2.5%	5	3.5%	-0.9%	-65.5%
Russia	10	2.4%	14	1.6%	+0.7%	-32.5%

Figure A.3. Malicious Activity by Source: Spam Zombies, 2014-2015

Geography	2015 Spam Rank	2015 Spam %	2014 Spam Rank	2014 Spam %	Annual Change	Change in Number of Attacks Originating from Geography
China	1	47.4%	11	3.4%	+44.0%	+255.0%
United States	2	8.5%	9	3.9%	+4.6%	-45.1%
Taiwan	3	5.2%	10	3.6%	+1.7%	-63.0%
Turkey	4	4.9%	40	0.5%	+4.5%	+176.1%
Italy	5	2.3%	12	3.2%	-0.9%	-81.8%
Hungary	6	2.2%	52	0.2%	+2.0%	+250.6%
Germany	7	2.0%	5	5.8%	-3.8%	-91.3%
Brazil	8	1.9%	13	2.1%	-0.2%	-77.1%
France	9	1.7%	41	0.4%	+1.2%	-5.5%
Canada	10	1.7%	42	0.4%	+1.3%	+6.3%

Figure A.4. Malicious Activity by Source: Phishing Hosts, 2014-2015

Geography	2015 Phishing Hosts Rank	2015 Phishing Hosts %	2014 Phishing Hosts Rank	2014 Phishing Hosts %	Annual Change	Change in Number of Attacks Originating from Geography
United States	1	50.8%	1	46.6%	+4.2%	+27.1%
Germany	2	4.7%	2	5.4%	-0.7%	+2.4%
United Kingdom	3	3.9%	3	3.9%	+0.1%	+18.9%
Hong Kong	4	3.4%	6	3.1%	+0.3%	+29.6%
Netherlands	5	3.3%	4	3.2%	+0.2%	+22.8%
France	6	3.2%	4	3.2%	+0.1%	+19.2%
Russia	7	2.3%	8	2.5%	-0.2%	+8.8%
Canada	8	2.2%	7	2.5%	-0.3%	+1.2%
China	9	1.9%	9	2.2%	-0.3%	+1.0%
Brazil	10	1.9%	11	2.0%	-0.2%	+5.5%

Figure A.5. Malicious Activity by Source: Bots, 2014-2015

Geography	2015 Bots Rank	2015 Bots %	2014 Bots Rank	2014 Bots %	Annual Change	Change in Number of Attacks Originating from Geography
China	1	46.1%	1	16.5%	+29.7%	+84.0%
United States	2	8.0%	2	16.1%	-8.1%	-67.4%
Taiwan	3	5.8%	3	8.5%	-2.6%	-54.8%
Turkey	4	4.5%	13	2.3%	+2.2%	+29.2%
Italy	5	2.4%	4	5.5%	-3.1%	-71.2%
Hungary	6	2.2%	5	4.9%	-2.6%	-69.7%
Germany	7	2.0%	8	3.1%	-1.1%	-58.0%
Brazil	8	2.0%	6	4.3%	-2.3%	-70.1%
France	9	1.7%	11	2.7%	-1.0%	-57.9%
Spain	10	1.7%	14	2.0%	-0.3%	-44.5%

Figure A.6. Malicious Activity by Source: Web Attack Origins, 2014-2015

Geography	2015 Web Attacking Countries Rank	2015 Web Attacking Countries %	2014 Web Attacking Countries Rank	2014 Web Attacking Countries %	Annual Change	Change in Number of Attacks Originating from Geography
United States	1	18.3%	1	21.1%	-2.8%	+80.9%
China	2	7.2%	2	6.6%	+0.5%	+125.2%
Netherlands	3	4.0%	5	2.3%	+1.7%	+261.1%
India	4	2.3%	6	1.1%	+1.2%	+319.6%
Brazil	5	1.6%	8	1.0%	+0.6%	+239.2%
Philippines	6	1.5%	7	1.1%	+0.5%	+196.6%
Vietnam	7	1.3%	20	0.4%	+0.9%	+586.6%
Japan	8	1.2%	4	3.2%	-1.9%	-19.2%
Egypt	9	1.1%	17	0.5%	+0.6%	+347.5%
Germany	10	1.1%	10	0.8%	+0.2%	+171.8%

Figure A.7. Malicious Activity by Source: Network Attack Origins, 2014-2015

Geography	2015 Network Attacking Countries Rank	2015 Network Attacking Countries %	2014 Network Attacking Countries Rank	2014 Network Attacking Countries %	Annual Change	Change in Number of Attacks Originating from Geography
China	1	29.1%	1	28.7%	+0.4%	-14.4%
United States	2	14.0%	2	16.6%	-2.6%	-28.9%
Netherlands	3	4.6%	3	4.2%	+0.4%	-7.5%
Russia	4	3.4%	4	3.2%	+0.2%	-9.6%
France	5	3.2%	6	2.6%	+0.6%	+3.7%
United Kingdom	6	3.1%	5	3.0%	+0.1%	-11.8%
Korea, South	7	2.6%	7	2.4%	+0.2%	-9.0%
India	8	2.4%	8	2.4%	-	-15.2%
Australia	9	2.2%	9	2.2%	-	-14.0%
Brazil	10	2.0%	11	2.1%	-0.1%	-17.7%

- In 2015, the United States and China remained the top two sources overall for malicious activity.
- The United States and China swap their positions as first and second in most of the six threat metrics, except for Malicious Code and Phishing Host, where India and Germany rank second respectively.

BOT-INFECTED COMPUTERS

Background

Bot-infected computer programs, or bots, are programs that are covertly installed on a user's machine in order to allow an attacker to control the targeted system remotely through a communication channel, such as Internet Relay Chat (IRC), P2P, or Hypertext Transfer Protocol (HTTP). These channels allow the remote attacker to control a large number of compromised computers over a single, reliable channel in a botnet, which can then be used to launch coordinated attacks.

Bots allow for a wide range of functionality, and most can be updated to assume new functionality by downloading new code and features. Attackers can use bots to perform a variety of tasks, such as setting up denial-of-service attacks against an organization's website, distributing spam and phishing attacks, distributing spyware and adware, propagating malicious code, and harvesting confidential information from compromised computers that may be used in identity theft—all of which can lead to serious financial and legal consequences. Attackers favor bot-infected computers with a decentralized Command and Control model because they are difficult to disable and allow the attackers to hide in plain sight among the massive amounts of unrelated traffic occurring over the same communication channels, such as P2P. Most important, botnet operations can be lucrative for their controllers because bots are also inexpensive and relatively easy to propagate.

Methodology

A bot-infected computer is considered active on a given day if it carries out at least one attack on that day. This does not have to be continuous; a single such computer can be active on a number of different days. A distinct bot-infected computer is one that was active at least once during the period. The bot-infected computer activities that Symantec tracks can be classified as active attacker bots or bots that send out spam, such as spam zombies.

Distributed denial-of-service (DDoS) campaigns may not always be indicative of bot-infected computer activity. DDoS activity can occur without the use of bot-infected computers. For example, the use of publicly available software such as "Low Orbit Ion Cannon", when used in a coordinated effort and in suffieciently large numbers, may disrupt some businesses' website operations.

The following analysis reveals the average lifespan of a bot-infected computer for the highest populations of bot-infected computers. To be included in the list, the geography must account for at least 0.1 percent of the global bot population.

Data and Commentary

Figure A.8. Table of Top 10 Bot Locations by Average Life Span of Bot, 2014-2015

Rank - 2015	Geography	Average Lifespan of Bot (Days) - 2015	% of World Bots - 2015	Average Lifespan of Bot (Days) - 2014	% of World Bots - 2014
1	United States	29	8.0%	21	16.1%
2	Switzerland	20	0.3%	10	0.2%
3	Indonesia	18	0.1%	15	0.2%
4	Romania	17	0.2%	23	0.2%
5	Egypt	16	0.1%	7	0.2%
6	Israel	16	0.8%	13	0.9%
7	Philippines	14	0.1%	10	0.2%
8	Greece	13	0.1%	7	0.3%
9	Bulgaria	12	0.2%	13	0.2%
10	Vietnam	12	0.1%	8	0.2%

- Bots located in United States were active for an average of 29 days in 2015, compared with 21 days in 2014; 8.0 percent of bots were located in Romania, compared with 16.1 percent in 2014.
- All other countries outside the top 10 had bot lifespan of 12 days or less. The overall global average bot lifespan was 8 days, slightly higher than in 2014, when it was 7.5 days.

APPENDIX B: SPAM AND FRAUD ACTIVITY TRENDS

This section covers phishing and spam trends. It also discusses activities observed on underground economy-type servers, as this is where much of the profit is made from phishing and spam attacks.

Phishing is an attempt by a third party to solicit confidential information from an individual, group, or organization by mimicking (or spoofing) a specific, usually well-known brand. Phishers attempt to trick users into disclosing personal data, such as credit card numbers, online banking credentials, and other sensitive information, which they can then use to commit fraudulent acts. Phishing generally requires victims to provide their credentials, often by duping them into filling out an online form. This is one of the characteristics that distinguish phishing from spam-based scams (such as the widely disseminated "419 scam" and other social engineering scams).

Spam is usually defined as junk or unsolicited email sent by a third party. While it is certainly an annoyance to users and administrators, spam is also a serious security concern because it can be used to deliver Trojans, viruses, and phishing attacks. Spam can also include URLs that link to malicious sites that, without the user's being aware of it, attack a user's system upon visitation. Large volumes of spam could also cause a loss of service or degradation in the performance of network resources and email services.

This section includes the following metrics:

- Analysis of spam activity by geography, industry sector, and company size
- Analysis of phishing activity by geography, industry sector, and company size

ANALYSIS OF SPAM ACTIVITY BY GEOGRAPHY, INDUSTRY SECTOR, AND COMPANY SIZE

Background

Spam activity trends can also reveal patterns that may be associated with particular geographical locations or hotspots. This may be a consequence of social and political changes in the region, such as increased broadband penetration and increased competition in the marketplace, which can drive down prices, thereby increasing adoption rates. There may also be other factors at work based on the local economic conditions. Similarly, the industry sector may also have an influence on an organization's risk factor, where certain industries may be exposed to different levels of threat by the nature of their business.

Moreover, the size of an organization can also play a part in determining it's exposure to risk. Small and medium sized businesses (SMBs) may find themselves the targets of spam attacks because they are perceived to be softer targets than larger organizations. They often have less stringent security countermeasures than larger organizations, which are more likely to apply greater resources to their antispam and security countermeasures.

Methodology

Analysis of spam activity based on geography, industry sector, and company size is based on the patterns of spam activity for Symantec.cloud clients for threats during 2015.

Data and Commentary

Figure B.1. Proportion of Email Traffic Identified as Spam by Industry Sector, 2015

Industry	Spam Rate
Mining	**56.3%**
Coal Mining	51.6%
Metal, Mining	63.6%
Nonmetallic Minerals, Except Fuels	55.0%
Oil & Gas Extraction	53.2%
Manufacturing	**54.2%**
Apparel & Other Textile Products	51.3%
Chemical & Allied Products	54.0%
Electronic & Other Electric Equipment	53.3%
Fabricated Metal Products	54.5%
Food & Kindred Products	53.5%
Furniture & Fixtures	54.4%
Industrial Machinery & Equipment	54.7%
Instruments & Related Products	53.5%
Leather & Leather Products	51.2%
Lumber & Wood Products	62.4%
Miscellaneous Manufacturing Industries	56.7%
Paper & Allied Products	52.6%
Petroleum & Coal Products	51.6%
Primary Metal Industries	61.3%
Printing & Publishing	55.5%
Rubber & Miscellaneous Plastics Products	52.9%
Stone, Clay, & Glass Products	52.9%
Textile Mill Products	57.5%
Tobacco Products	58.6%
Transportation Equipment	51.1%
Construction	**53.7%**
General Building Contractors	54.4%
Heavy Construction, Except Building	53.4%
Special Trade Contractors	53.4%
Services	**53.0%**
Amusement & Recreation Services	52.3%
Auto Repair, Services, & Parking	52.6%
Business Services	52.7%
Educational Services	55.1%
Engineering & Management Services	52.6%
Health Services	54.1%
Hotels & Other Lodging Places	53.1%
Legal Services	54.0%
Membership Organizations	53.3%
Miscellaneous Repair Services	53.4%
Motion Pictures	53.9%
Museums, Botanical, Zoological Gardens	54.0%
Personal Services	53.7%
Private Households	49.4%
Services, Not Elsewhere Classified	51.9%
Social Services	52.5%
Agriculture, Forestry, & Fishing	**52.9%**
Agricultural Production - Crops	52.0%
Agricultural Production - Livestock	55.7%
Agricultural Services	52.9%
Fishing, Hunting, & Trapping	51.2%
Forestry	53.2%
Retail Trade	**52.7%**
Apparel & Accessory Stores	54.8%
Automotive Dealers & Service Stations	51.9%
Building Materials & Gardening Supplies	52.3%
Eating & Drinking Places	52.6%
Food Stores	51.4%
Furniture & Home Furnishings Stores	51.3%
General Merchandise Stores	51.0%
Miscellaneous Retail	53.3%
Non-Classifiable Establishments	**52.6%**
Non-Classifiable Establishments	52.6%
Wholesale Trade	**52.5%**
Wholesale Trade - Durable Goods	53.3%

Wholesale Trade – Nondurable Goods	51.7%
Public Administration	**52.2%**
Administration of Economic Programs	51.1%
Administration of Human Resources	51.1%
Environmental Quality & Housing	52.4%
Executive, Legislative, & General	52.7%
Finance, Taxation, & Monetary Policy	52.2%
Justice, Public Order, & Safety	52.3%
National Security & International Affairs	52.7%
Finance, Insurance, & Real Estate	**52.1%**
Depository Institutions	52.2%
Holding & Other Investment Offices	52.0%
Insurance Agents, Brokers, & Service	51.7%
Insurance Carriers	51.9%
Non-Depository Institutions	52.4%
Real Estate	52.1%
Security & Commodity Brokers	51.7%
Transportation & Public Utilities	**51.8%**
Communications	51.6%
Electric, Gas, & Sanitary Services	54.1%
Local & Interurban Passenger Transit	53.8%
Pipelines, Except Natural Gas	50.3%
Railroad Transportation	55.1%
Transportation by Air	50.3%
Transportation Services	50.4%
Trucking & Warehousing	51.5%
U.S. Postal Service	57.8%
Water Transportation	52.8%
Other Non-SIC Related Industries	
Energy	**53.0%**
Electric, Gas, & Sanitary Services	54.1%
Oil & Gas Extraction	53.2%
Coal Mining	51.6%

Figure B.2. Proportion of Email Traffic Identified as Spam by Organization Size, 2015

Company Size	Spam Rate
1-250	52.9%
251-500	53.3%
501-1000	53.3%
1001-1500	51.9%
1501-2500	52.6%
2501+	52.5%

Figure B.3. Proportion of Email Traffic Identified as Spam by Geographic Location, 2015

Geography	Spam Rate
Sri Lanka	68.7%
Brazil	62.5%
Kuwait	59.2%
Poland	58.8%
India	57.6%
Papua New Guinea	57.0%
Mexico	56.8%
Indonesia	55.9%
Taiwan	55.7%
Hungary	55.4%

- The spam rate decreased across all top 10 geographies in 2015. The highest rate of spam was for organizations in Sri Lanka, with an overall average spam rate of 68.7 percent.
- The spam rate slightly decreased across all top 10 industry sectors in 2015, with Mining on the top at 56.3 percent (the same as in 2014).
- The spam rate slightly decreased for all sizes of organizations in 2015.

ANALYSIS OF PHISHING ACTIVITY BY GEOGRAPHY, INDUSTRY SECTOR, AND COMPANY SIZE

Background

Phishing activity trends can also reveal patterns that may be associated with particular geographical locations or hotspots. For example, the industry sector may also have an influence on an organization's risk factor, where certain industries may be exposed to different levels of threat by the nature of their business.

Moreover, the size of an organization can also play a part in determining its exposure to risk. Small- to medium-sized businesses (SMBs) may find themselves the targets of spam attacks because SMBs are perceived to be softer targets, as they are less likely to have the same levels of defense in depth as larger organizations, which tend to have greater budgetary expenditure applied to antispam and security countermeasures.

Methodology

Analysis of phishing activity based on geography, industry sector, and company size is based on the patterns of spam activity for Symantec.cloud clients for threats during 2015.

Data and Commentary

Figure B.4. Proportion of Email Traffic Identified as Phishing by Industry Sector, 2015

Industry	Phishing Rate
Transportation & Public Utilities	**1 in 2,948**
Communications	1 in 3,053
Electric, Gas, & Sanitary Services	1 in 3,079
Local & Interurban Passenger Transit	1 in 4,056
Pipelines, Except Natural Gas	1 in 11,366
Railroad Transportation	1 in 751
Transportation by Air	1 in 4,328
Transportation Services	1 in 2,595
Trucking & Warehousing	1 in 2,084
U.S. Postal Service	1 in 4,825
Water Transportation	1 in 1,692
Construction	**1 in 2,349**
General Building Contractors	1 in 2,233
Heavy Construction, Except Building	1 in 3,064
Special Trade Contractors	1 in 2,119
Wholesale Trade	**1 in 2,226**
Wholesale Trade - Durable Goods	1 in 2,046
Wholesale Trade - Nondurable Goods	1 in 2,463
Mining	**1 in 2,225**
Coal Mining	1 in 2,108
Metal, Mining	1 in 2,333
Nonmetallic Minerals, Except Fuels	1 in 750
Oil & Gas Extraction	1 in 2,387
Finance, Insurance, & Real Estate	**1 in 2,200**
Depository Institutions	1 in 2,034
Holding & Other Investment Offices	1 in 2,319
Insurance Agents, Brokers, & Service	1 in 4,145
Insurance Carriers	1 in 2,045

Non-Depository Institutions	1 in 1,606
Real Estate	1 in 1,785
Security & Commodity Brokers	1 in 5,644
Manufacturing	**1 in 1,999**
Apparel & Other Textile Products	1 in 1,942
Chemical & Allied Products	1 in 2,118
Electronic & Other Electric Equipment	1 in 2,675
Fabricated Metal Products	1 in 549
Food & Kindred Products	1 in 2,452
Furniture & Fixtures	1 in 722
Industrial Machinery & Equipment	1 in 2,654
Instruments & Related Products	1 in 2,952
Leather & Leather Products	1 in 3,302
Lumber & Wood Products	1 in 1,216
Miscellaneous Manufacturing Industries	1 in 1,644
Paper & Allied Products	1 in 3,028
Petroleum & Coal Products	1 in 2,570
Primary Metal Industries	1 in 3,256
Printing & Publishing	1 in 1,071
Rubber & Miscellaneous Plastics Products	1 in 2,998
Stone, Clay, & Glass Products	1 in 1,781
Textile Mill Products	1 in 910
Tobacco Products	1 in 3,271
Transportation Equipment	1 in 5,446
Services	**1 in 1,717**
Amusement & Recreation Services	1 in 1,688
Auto Repair, Services, & Parking	1 in 2,529
Business Services	1 in 2,010
Educational Services	1 in 982
Engineering & Management Services	1 in 1,570
Health Services	1 in 2,711
Hotels & Other Lodging Places	1 in 1,771
Legal Services	1 in 1,151
Membership Organizations	1 in 1,237
Miscellaneous Repair Services	1 in 3,195
Motion Pictures	1 in 2,617
Museums, Botanical, Zoological Gardens	1 in 1,126
Personal Services	1 in 4,490
Private Households	1 in 1,378
Services, Not Elsewhere Classified	1 in 2,160
Social Services	1 in 2,027
Non-Classifiable Establishments	**1 in 1,708**
Non-Classifiable Establishments	1 in 1,708
Agriculture, Forestry, & Fishing	1 in 1,229
Agricultural Production - Crops	1 in 2,230
Agricultural Production - Livestock	1 in 1,167
Agricultural Services	1 in 890
Fishing, Hunting, & Trapping	1 in 3,702
Forestry	1 in 2,237
Public Administration	**1 in 1,198**
Administration of Economic Programs	1 in 3,491
Administration of Human Resources	1 in 5,403
Environmental Quality & Housing	1 in 1,897
Executive, Legislative, & General	1 in 849
Finance, Taxation, & Monetary Policy	1 in 5,025
Justice, Public Order, & Safety	1 in 827
National Security & International Affairs	1 in 3,912
Retail Trade	**1 in 690**
Apparel & Accessory Stores	1 in 2,764
Automotive Dealers & Service Stations	1 in 1,841
Building Materials & Gardening Supplies	1 in 1,349
Eating & Drinking Places	1 in 2,171
Food Stores	1 in 1,387
Furniture & Home Furnishings Stores	1 in 1,681
General Merchandise Stores	1 in 2,817
Miscellaneous Retail	1 in 338

Other Non-SIC Related Industries	
Energy	**1 in 2,525**
Coal Mining	1 in 2,108
Oil & Gas Extraction	1 in 2,387
Electric, Gas, & Sanitary Services	1 in 3,079

Figure B.5. Proportion of Email Traffic Identified as Phishing by Organization Size, 2015

Company Size	Phishing Rate
1-250	1 in 1,548
251-500	1 in 758
501-1000	1 in 1,734
1001-1500	1 in 2,212
1501-2500	1 in 1,601
2501+	1 in 2,862

Figure B.6. Proportion of Email Traffic Identified as Phishing by Geographic Location, 2015

Country	Phishing Rate
Hungary	1 in 812
South Africa	1 in 900
Brazil	1 in 1,128
Austria	1 in 1,147
United Kingdom	1 in 1,148
Netherlands Antilles	1 in 1,241
Philippines	1 in 1,411
New Zealand	1 in 1,681
Ireland	1 in 1,746
United Arab Emirates	1 in 1,846

- The highest average rate for phishing activity in 2015 was for organizations in Hungary, with an overall average phishing rate of 1 in 812.0, which didn't even appear in the top 10 in 2014.
- Organizations in the Transportation & Public Utilities sector were subjected to the highest level of phishing activity in 2015, with 1 in 2,948.0 emails identified and blocked as a phishing attack. In 2014, the sector with the highest average phishing rate was the Agriculture sector, with a phishing rate of 1 in 833.4.
- The phishing rate decreased for most of the sizes of organization in 2015. Of all emails sent to large enterprises with more than 2,500 employees in 2015, 1 in 2,862 was identified and blocked as a phishing attack, compared with 1 in 1,685.4 in 2014.
- Of all emails sent to businesses with up to 250 employees in 2015, 1 in 1,548 was identified and blocked as a phishing attack, compared with 1 in 1,401.5 in 2014.

ANALYSIS OF MALICIOUS CODE ACTIVITY BY GEOGRAPHY, INDUSTRY SECTOR, AND COMPANY SIZE

Background

Malicious code activity trends can also reveal patterns that may be associated with particular geographical locations or hotspots. This may be a consequence of social and political changes in the region, such as increased broadband penetration and increased competition in the marketplace that can drive down prices, increasing adoption rates. There may be other factors at work based on the local economic conditions that present different risk factors. Similarly, the industry sector may also have an influence on an organization's risk factor, where certain industries may be exposed to different levels of threat by the nature of their business.

Moreover, the size of an organization can also play a part in determining their exposure to risk. Small- to medium-sized businesses (SMBs) may find themselves the target of a malicious attack by virtue of the relationships they have with other organizations. For example, a company may be subjected to an attack because they are a supplier to a larger organization, and attackers may seek to take advantage of this relationship in forming the social engineering behind subsequent attacks to the main target using the SMB as a springboard for these later attacks. SMBs are perceived to be a softer target; they are less likely to have the same levels of security as a larger organization, which will often have a larger budget applied to their security countermeasures.

Methodology

Analysis of malicious code activity on geography, industry, and size are based on the telemetry analysis from Symantec.cloud clients for threats detected and blocked against those organizations in email traffic during 2015.

This analysis looked at the profile of organizations being subjected to malicious attacks in contrast to the source of the attack.

Data and Commentary

Figure B.7. Proportion of Email Traffic Identified as Malicious by Industry Sector, 2015

Industry	Malware Rate
Retail Trade	**1 in 74**
Apparel & Accessory Stores	1 in 275
Automotive Dealers & Service Stations	1 in 169
Building Materials & Gardening Supplies	1 in 232
Eating & Drinking Places	1 in 301
Food Stores	1 in 106
Furniture & Home Furnishings Stores	1 in 213
General Merchandise Stores	1 in 271
Miscellaneous Retail	1 in 36
Public Administration	**1 in 151**
Administration of Economic Programs	1 in 551
Administration of Human Resources	1 in 1,263
Environmental Quality & Housing	1 in 306
Executive, Legislative, & General	1 in 103
Finance, Taxation, & Monetary Policy	1 in 892
Justice, Public Order, & Safety	1 in 100
National Security & International Affairs	1 in 469
Agriculture, Forestry, & Fishing	**1 in 187**
Agricultural Production - Crops	1 in 290
Agricultural Production - Livestock	1 in 130
Agricultural Services	1 in 157
Fishing, Hunting, & Trapping	1 in 508
Forestry	1 in 359
Services	**1 in 199**
Amusement & Recreation Services	1 in 184
Auto Repair, Services, & Parking	1 in 248
Business Services	1 in 245
Educational Services	1 in 115
Engineering & Management Services	1 in 159
Health Services	1 in 396

Hotels & Other Lodging Places	1 in 186
Legal Services	1 in 164
Membership Organizations	1 in 138
Miscellaneous Repair Services	1 in 407
Motion Pictures	1 in 260
Museums, Botanical, Zoological Gardens	1 in 57
Personal Services	1 in 502
Private Households	1 in 176
Services, Not Elsewhere Classified	1 in 254
Social Services	1 in 231
Wholesale Trade	**1 in 234**
Wholesale Trade - Durable Goods	1 in 208
Wholesale Trade - Nondurable Goods	1 in 271
Construction	**1 in 240**
General Building Contractors	1 in 216
Heavy Construction, Except Building	1 in 306
Special Trade Contractors	1 in 231
Manufacturing	**1 in 243**
Apparel & Other Textile Products	1 in 189
Chemical & Allied Products	1 in 270
Electronic & Other Electric Equipment	1 in 336
Fabricated Metal Products	1 in 73
Food & Kindred Products	1 in 275
Furniture & Fixtures	1 in 70
Industrial Machinery & Equipment	1 in 269
Instruments & Related Products	1 in 333
Leather & Leather Products	1 in 292
Lumber & Wood Products	1 in 141
Miscellaneous Manufacturing Industries	1 in 191
Paper & Allied Products	1 in 351
Petroleum & Coal Products	1 in 303
Primary Metal Industries	1 in 396
Printing & Publishing	1 in 155
Rubber & Miscellaneous Plastics Products	1 in 322
Stone, Clay, & Glass Products	1 in 174
Textile Mill Products	1 in 96
Tobacco Products	1 in 575
Transportation Equipment	1 in 548
Non-Classifiable Establishments	**1 in 277**
Non-Classifiable Establishments	1 in 277
Mining	**1 in 304**
Coal Mining	1 in 157
Metal, Mining	1 in 333
Nonmetallic Minerals, Except Fuels	1 in 98
Oil & Gas Extraction	1 in 340
Finance, Insurance, & Real Estate	**1 in 310**
Depository Institutions	1 in 398
Holding & Other Investment Offices	1 in 256
Insurance Agents, Brokers, & Service	1 in 562
Insurance Carriers	1 in 274
Non-Depository Institutions	1 in 176
Real Estate	1 in 206
Security & Commodity Brokers	1 in 541
Transportation & Public Utilities	**1 in 338**
Communications	1 in 382
Electric, Gas, & Sanitary Services	1 in 459
Local & Interurban Passenger Transit	1 in 448
Pipelines, Except Natural Gas	1 in 1,379
Railroad Transportation	1 in 72
Transportation by Air	1 in 454
Transportation Services	1 in 240
Trucking & Warehousing	1 in 229
U.S. Postal Service	1 in 628
Water Transportation	1 in 163

Other Non-SIC Related Industries	
Energy	**1 in 319**
Coal Mining	1 in 157
Oil & Gas Extraction	1 in 340
Electric, Gas, & Sanitary Services	1 in 459

Figure B.8. Proportion of Email Traffic Identified as Malicious by Organization Size, 2015

Company Size	Malware Rate
1-250	1 in 184
251-500	1 in 82
501-1000	1 in 189
1001-1500	1 in 312
1501-2500	1 in 168
2501+	1 in 352

Figure B.9. Proportion of Email Traffic Identified as Malicious - by Geographic Location, 2015

Country	Malware Rate
Hungary	1 in 86
United Kingdom	1 in 112
Austria	1 in 124
Netherlands Antilles	1 in 140
Brazil	1 in 162
Hong Kong	1 in 176
United Arab Emirates	1 in 199
South Africa	1 in 217
Indonesia	1 in 236
Philippines	1 in 241

- Hungary has appeared in the top 10 list of email threats, especially ranking first with malware and phish attacks.
- Globally, organizations in the Retail Trade sector were subjected to the highest level of malicious attacks in email traffic, with 1 in 74 emails blocked as malicious in 2015, which didn't appear in top 10 list for 2014.
- Malicious email threats have slightly decreased for all sizes of organizations, with 1 in 352 emails being blocked as malicious for large enterprises with more than 2,500 employees in 2015, compared with 1 in 284.7 in 2014.
- One in 184 emails were blocked as malicious for small to medium-sized businesses with between 1-250 employees in 2015, compared with 1 in 142.3 in 2014. ■

APPENDIX C: VULNERABILITY TRENDS

A vulnerability is a weakness that allows an attacker to compromise the availability, confidentiality, or integrity of a computer system. Vulnerabilities may be the result of a programming error or a flaw in the design that will affect security.

Vulnerabilities can affect both software and hardware. It is important to stay abreast of new vulnerabilities identified in the threat landscape because early detection and patching will minimize the chances of being exploited. This section discusses selected vulnerability trends, providing analysis and discussion of the trends indicated by the data.

The following metrics are included:

- Zero-Day Vulnerabilities
- ICS Vulnerabilities

ZERO-DAY VULNERABILITIES

Background

Zero-day vulnerabilities are vulnerabilities against which no vendor has released a patch. The absence of a patch for a zero-day vulnerability presents a threat to organizations and consumers alike, because in many cases these threats can evade purely signature-based detection until a patch is released. The unexpected nature of zero-day threats is a serious concern, especially because they may be used in targeted attacks and in the propagation of malicious code.

Methodology

Zero-day vulnerabilities are a sub-set of the total number of vulnerabilities documented over the reporting period. A zero-day vulnerability is one that is exploitable, or appears to have been exploited in the wild *prior* to being publicly known. It may not have been known to the affected vendor prior to exploitation, and at the time of the exploit activity, the vendor had not released a patch. The data for this section consists of the vulnerabilities Symantec has identified that meet the above criteria.

Data and Commentary

Figure C.1: Zero-Day Vulnerabilities Identified in 2015

BID #	Description
72261	Adobe Flash Player CVE-2015-0310 Unspecified Memory Corruption Vulnerability
72283	Adobe Flash Player CVE-2015-0311 Use After Free Memory Corruption Vulnerability
72325	GNU glibc CVE-2015-0235 Remote Heap Buffer Overflow Vulnerability
72429	Adobe Flash Player CVE-2015-0313 Remote Code Execution Vulnerability
72693	Komodia Redirector SSL Certificate Validation Spoofing Vulnerability
72711	Samba 'TALLOC_FREE()' Function Remote Code Execution Vulnerability
73235	OpenSSL CVE-2015-0291 Denial of Service Vulnerability
73356	Multiple ANTlabs Products CVE-2015-0932 Arbitrary File Access Vulnerability
73995	Microsoft Office CVE-2015-1641 Memory Corruption Vulnerability
74334	WordPress Comment Section HTML Injection Vulnerability
74062	Adobe Flash Player Multiple Unspecified Memory Corruption Vulnerabilities
74013	Microsoft Windows HTTP Protocol Stack CVE-2015-1635 Remote Code Execution Vulnerability
74245	Microsoft Windows CVE-2015-1701 Local Privilege Escalation Vulnerability
74640	QEMU 'hw/block/fdc.c' VENOM Remote Memory Corruption Vulnerability
75371	Adobe Flash Player CVE-2015-3113 Unspecified Heap Buffer Overflow Vulnerability
75347	SwiftKey CVE-2015-4640 Man in The Middle Security Bypass Vulnerability
75353	SwiftKey CVE-2015-4641 Directory Traversal Vulnerability
75308	Apple Mac OS X and iOS XARA Multiple Security Vulnerabilities
75818	Oracle Java SE CVE-2015-2590 Remote Security Vulnerability
75745	Microsoft Internet Explorer CVE-2015-2425 Remote Memory Corruption Vulnerability
75951	Microsoft Windows OpenType Font Driver CVE-2015-2426 Remote Code Execution Vulnerability
75568	Adobe Flash Player ActionScript 3 ByteArray Use After Free Remote Memory Corruption Vulnerability
75712	Adobe Flash Player CVE-2015-5122 Use After Free Remote Memory Corruption Vulnerability
75710	Adobe Flash Player ActionScript 3 BitmapData Use After Free Remote Memory Corruption Vulnerability
76357	Rockwell Automation 1766-L32 Series Products Remote File Include Vulnerability
76332	Prisma Web Products Cross Site Request Forgery and Security Bypass Vulnerabilities
76327	Schneider Electric Modicon M340 PLC Station P34 Module Modicon Multiple Security Vulnerabilities
76330	Moxa ioLogik E2210 ICS-ALERT-15-224-04 Multiple Security Vulnerabilities
76323	KAKO HMI Hardcoded Password Security Bypass Vulnerability
76370	Google Admin For Android Sandbox Security Bypass Vulnerability
76249	Mozilla Firefox CVE-2015-4495 Same Origin Policy Security Bypass Vulnerability
76637	Multiple FireEye Appliances Multiple Security Vulnerabilities
76675	Mozilla Bugzilla Unauthorized Access Vulnerability
76672	Advantech WebAccess CVE-2014-9208 Multiple Stack Buffer Overflow Vulnerabilities
76608	Microsoft Windows Kernel Mode Driver CVE-2015-2546 Local Privilege Escalation Vulnerability
76667	Microsoft Office CVE-2015-2545 Remote Code Execution Vulnerability
76594	Microsoft Windows Media Center CVE-2015-2509 Remote Code Execution Vulnerability
76694	Hancom Hangul Word Processor CVE-2015-6585 Type Confusion Remote Code Execution Vulnerability
76421	Apple Mac OS X Multiple Privilege Escalation Vulnerabilities
76956	WinRAR SFX 'Text and Icon' Function Remote Code Execution Vulnerability
77012	Avast Antivirus X.509 Certificate Remote Code Execution Vulnerability
77087	MAGMI Plugin For Magento 'download_file.php' Directory Traversal Vulnerability
77038	Multiple ZHONE Routers Multiple Security Vulnerabilities
77320	SolarWinds Log and Event Manager XML External Entity Injection Vulnerability
77081	Adobe Flash Player CVE-2015-7645 Remote Code Execution Vulnerability

77558	IBM Installation Manager '/tmp' Local Command Injection Vulnerability
77389	vBulletin Unspecified Security Vulnerability
77521	Apache Commons Collections 'InvokerTransformer.java' Remote Code Execution Vulnerability
78503	Multiple ZTE/Huawei/Gemtek/Quanta Products Multiple Unspecified Security Vulnerabilities
78809	Multiple FireEye Products 'JAR Analysis' Remote Code Execution Vulnerability
79195	Joomla! Core CVE-2015-8562 Remote Code Execution Vulnerability
79358	GNU GRUB2 CVE-2015-8370 Multiple Local Authentication Bypass Vulnerabilities
79705	Adobe Flash Player and AIR CVE-2015-8651 Unspecified Integer Overflow Vulnerability

For further details on the BID references,

- In 2015, Symantec saw an increase in number of zero-day vulnerabilities compared to 2014.
- There was a 125 percent increase in the number of exploitable zero-day vulnerabilities in 2015 compared with 2014.

ICS VULNERABILITIES

Background

This metric will examine all the vulnerabilities within Industrial Control Systems (ICS) technologies. ICS is a general term that encompasses several types of control systems used in industrial production, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other smaller control system configurations such as programmable logic controllers (PLC) often found in the industrial sectors and critical infrastructures. ICSs are typically used in industries such as electrical, water, oil, gas and data. Based on data received from remote stations, automated or operator-driven supervisory commands can be pushed to remote station control devices.

SCADA represents a wide range of protocols and technologies for monitoring and managing equipment and machinery in various sectors of critical infrastructure and industry. This includes, but is not limited to, power generation, manufacturing, oil and gas, water treatment, and waste management. The security of SCADA technologies and protocols is a concern related to national security because the disruption of related services can result in, among other things, the failure of infrastructure and potential loss of life.

Methodology

This discussion is based on data surrounding publicly known vulnerabilities affecting ICS technologies. The purpose of the metric is to provide insight into the state of security research in relation to ICS technologies. Vulnerabilities affecting ICS may present a threat to critical infrastructure that relies on these systems. Due to the potential for disruption of critical services, these vulnerabilities may be associated with politically motivated or state-sponsored attacks. This is a concern for both governments and enterprises involved in the critical infrastructure sector. While this metric provides insight into public ICS/SCADA vulnerability disclosures, due to the sensitive nature of vulnerabilities affecting critical infrastructure it is likely that private security research is conducted by ICS technology and security vendors. Symantec does not have insight into any private research because the results of sduch research are not publicly disclosed.

Data and Commentary

Figure C.2: ICS Vulnerabilities Identified in 2015

BID #	Description
71951	Schneider Electric Wonderware InTouch Access Anywhere Server Buffer Overflow Vulnerability
72066	Multiple General Electric (GE) Products Unspecified Denial-of-Service Vulnerability
72069	Multiple General Electric (GE) Products Hardcoded Key Security Bypass Vulnerability
72065	Multiple Siemens SIMATIC WinCC Products Local Security Bypass Vulnerability
72073	Multiple Siemens SIMATIC WinCC Products Local Security Bypass Vulnerability
72075	Multiple Siemens SIMATIC WinCC Products Local Security Bypass Vulnerability
72096	GE Proficy HMI/SCADA CIMPLICITY CimView Memory Access Violation
72254	Schneider Electric ETG3000 FactoryCast HMI Gateway Vulnerabilities
72250	Siemens SCALANCE X-300/X408 Switch Family DOS Vulnerabilities
72251	Siemens SCALANCE X-300/X408 Switch Family DOS Vulnerabilities
72258	Schneider Electric ETG3000 FactoryCast HMI Gateway Vulnerabilities
72282	Siemens SIMATIC S7-1200 CPU Web Vulnerability
72335	Schneider Electric Multiple Products Buffer Overflow Vulnerability
72512	Siemens SCALANCE X-200IRT Switch Family User Impersonation Vulnerability
72521	Siemens Ruggedcom WIN Vulnerability
72522	Siemens Ruggedcom WIN Vulnerability
72523	Siemens Ruggedcom WIN Vulnerability
72691	Siemens SIMATIC STEP 7 TIA Portal Vulnerabilities
72695	Siemens SIMATIC STEP 7 TIA Portal Vulnerabilities
72764	Schneider Electric DTM Stack Buffer Overflow Vulnerability
72971	Siemens SPCanywhere CVE-2015-1599 Authentication Bypass Vulnerability
72973	Siemens SIMATIC S7-300 CPU Denial-of-Service Vulnerability
72976	Siemens SPC Controller Series Denial-of-Service Vulnerability
72970	SPCanywhere Information Disclosure Vulnerability
72972	SPCanywhere SSL Certificate Validation Security Bypass Vulnerability
72974	SPCanywhere Code Injection Vulnerability
72975	SPCanywhere Local Information Disclosure Vulnerability
72979	Siemens SIMATIC ProSave, SIMATIC CFC, SIMATIC STEP 7, SIMOTION Scout, and STARTER Insufficiently Qualified Paths
73026	GE Hydran M2 Predictable TCP Initial Sequence Vulnerability
73096	Schneider Electric Pelco DS-NVs Buffer Overflow Vulnerability
73179	CVE-2014-5427
73181	CVE-2014-5428
73177	CVE-2015-0984
73180	CVE-2015-0985
73247	Rockwell Automation FactoryTalk DLL Hijacking Vulnerabilities
73378	Multiple Schneider Electric Products Information Disclosure Vulnerability
73387	Schneider Electric InduSoft Web Studio and InTouch Machine Edition 2014 Vulnerabilities
73386	Multiple Schneider Electric Products Brute Force Authentication Bypass Vulnerability
73389	Multiple Schneider Electric Products Local Information Disclosure Vulnerability
73472	Ecava Integraxor SCADA Server Multiple Local Code Execution Vulnerabilities
73960	Moxa VPort ActiveX SDK Plus Stack-Based Buffer Overflow Vulnerability
74040	Multiple Siemens SIMATIC Products Authentication Bypass Vulnerability
74028	Multiple Siemens SIMATIC Products Denial of Service Vulnerability
74553	Rockwell Automation RSLinx Classic Vulnerability
74772	Schneider Electric OPC Factory Server DLL Loading Arbitrary Code Execution Vulnerability
74966	Moxa SoftCMS Buffer Overflow Vulnerability
75100	Sinapsi eSolar Light Plaintext Passwords Vulnerability
75297	Schneider Electric Wonderware System Platform Vulnerabilities
75427	Siemens Climatix BACnet/IP Communication Module Cross-site Scripting Vulnerability
75904	Siemens SICAM MIC Authentication Bypass Vulnerability

75982	Siemens RuggedCom ROS and ROX-based Devices TLS POODLE Vulnerability
76307	Schneider Electric IMT25 DTM Vulnerability
76330	Moxa ioLogik E2210 Vulnerabilities
76332	Prisma Web Vulnerabilities
76327	Schneider Electric Modicon M340 PLC Station P34 Module Vulnerabilities
76323	KAKO HMI Hard-coded Password
76355	Rockwell Automation 1769-L18ER and A LOGIX5318ER Vulnerability
76357	Rockwell Automation 1766-L32 Series Vulnerability
76507	Siemens SIMATIC S7-1200 CSRF Vulnerability
76546	Siemens RUGGEDCOM ROS IP Forwarding Vulnerability
76617	SMA Solar Technology AG Sunny WebBox Hard-coded Account Vulnerability
76612	Moxa Industrial Managed Switch Vulnerabilities
76613	Schneider Electric Modicon PLC Vulnerabilities
76614	Cogent DataHub Code Injection Vulnerability
76672	Advantech WebAccess Buffer Overflow Vulnerability
76709	Yokogawa Multiple Products Buffer Overflow Vulnerabilities
76753	Advantech WebAccess Local Stack Buffer Overflow Vulnerability
76756	Multiple GE MDS PulseNET Products Multiple Security vulnerabilities
76754	CODESYS Gateway Server Multiple Heap Buffer Overflow Vulnerabilities
75993	Harman-Kardon Uconnect Vulnerability
76820	Everest Software PeakHMI Pointer Dereference Vulnerabilities
76822	Resource Data Management Privilege Escalation Vulnerability
76825	IBC Solar ServeMaster Source Code Vulnerability
76846	Endress+Hauser Fieldcare/CodeWrights HART Comm DTM XML Injection Vulnerability
76845	EasyIO-30P-SF Hard-Coded Credential Vulnerability
76938	Omron Multiple Product Vulnerabilities
76936	Omron Multiple Product Vulnerabilities
77075	Nordex NC2 XSS Vulnerability
77109	SDG Technologies Plug and Play SCADA XSS Vulnerability
77107	3S CODESYS Runtime Toolkit Null Pointer Dereference Vulnerability
77256	IniNet Solutions embedded WebServer Cleartext Storage Vulnerability
77258	3S CODESYS Gateway Null Pointer Exception Vulnerability
77259	IniNet Solutions SCADA Web Server Vulnerabilities
77291	Janitza UMG Power Quality Measuring Products Vulnerabilities
77332	Siemens RuggedCom Improper Ethernet Frame Padding Vulnerability
77331	Infinite Automation Systems Mango Automation Vulnerabilities
77333	Rockwell Automation Micrologix 1100 and 1400 PLC Systems Vulnerabilities
77498	Advantech EKI Hard-coded SSH Keys Vulnerability
77571	Unitronics VisiLogic OPLC IDE Vulnerabilities
77630	Exemys Web Server Bypass Vulnerability
77658	Tibbo AggreGate Platform Vulnerabilities
76935, 76934	Moxa OnCell Central Manager Vulnerabilities
77819	Moxa OnCell Central Manager Vulnerabilities
78345	Siemens SIMATIC Communication Processor Vulnerability
78421	Schneider Electric ProClima ActiveX Control Vulnerabilities
79622	Schneider Electric Modicon M340 Buffer Overflow Vulnerability
77287, 77283, 77280, 77312	Siemens RUGGEDCOM ROX-based Devices NTP Vulnerabilities

Please note that some BIDs refer to more than one vulnerability. For full details on the BID references listed here, please visit securityfocus.com.

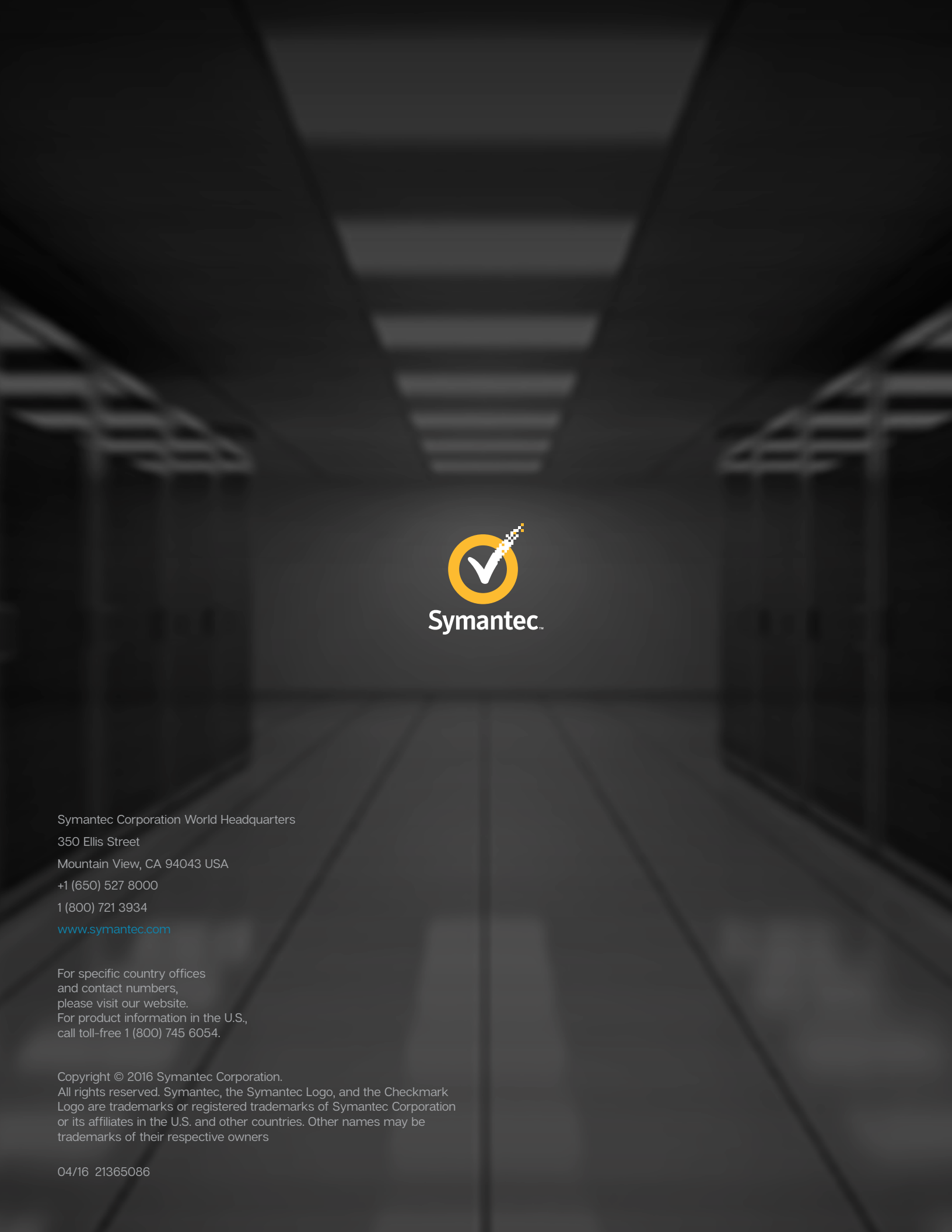
- The number of ICS vulnerabilities tremendously increased in 2015. In 2015, there were at least 135 public vulnerabilities, an increase compared with 35 ICS related vulnerabilities disclosed in 2014. ■

ABOUT SYMANTEC

Symantec Corporation is the global leader in cybersecurity. Operating one of the world's largest cyber intelligence networks, we see more threats, and protect more customers from the next generation of attacks. We help companies, governments and individuals secure their most important data wherever it lives.

MORE INFORMATION

- Symantec Worldwide: http://www.symantec.com/
- ISTR and Symantec Intelligence Resources: http://www.symantec.com/threatreport/
- Symantec Security Response: http://www.symantec.com/security_response/
- Norton Threat Explorer: http://us.norton.com/security_response/threatexplorer/



Symantec Corporation World Headquarters

350 Ellis Street

Mountain View, CA 94043 USA

+1 (650) 527 8000

1 (800) 721 3934

www.symantec.com

For specific country offices
and contact numbers,
please visit our website.
For product information in the U.S.,
call toll-free 1 (800) 745 6054.

04/16 21365086