Symantec Intelligence Report: November 2012

A look at identities lost in data breaches; Holiday spam

Welcome to the November edition of the Symantec Intelligence report, which provides the latest analysis of cyber security threats, trends, and insights from the Symantec Intelligence team concerning malware, spam, and other potentially harmful business risks. The data used to compile the analysis for this report includes data from January through November 2012.

Report highlights

- Spam – 68.8 percent (an increase of 4.0 percentage points since October): page 6
- Phishing – One in 445.1 emails identified as phishing (a decrease of 0.124 percentage points since October): page 9
- Malware – One in 255.8 emails contained malware (an decrease of 0.05 percentage points since October): page 10
- Malicious websites – 1,847 websites blocked per day (an increase of 97.9 percent since October): page 12
- A look at identities lost in data breaches: page 2
- Spam as a holiday tradition: page 4

Introduction

In this month's Symantec Intelligence Report, we take a second look at data breaches this year. However, instead of looking at the trends in terms of the nature of the breaches, we examine the types of data that is often stolen during a data breach. It turns out the most commonly stolen information is more personal than you might first expect.

We also take a look at spam during this holiday season. We've noticed that spammers are using the holidays as a means to entice users to check out the wares they're peddling, in much the same way they have in years past. There has also been an increase in the size of spam email messages this month—messages 10kb and larger are up 21 percent, from 17.3 percent in October to 38.3 percent of all spam email in November. We take a look at why this is, and what we see in store for the rest of the month.

I hope you enjoy reading this month's edition of the report, and please feel free to contact me directly with any comments or feedback.

Ben Nahorney, Cyber Security Threat Analyst
symantec_intelligence@symantec.com

@symantec, @symanteccloud, @norton, @threatintel

Report analysis

Information exposed: A look at identities lost in data breaches

By Ben Nahorney, Cyber Security Threat Analyst, Symantec

Back in the August report we took a look at data breaches, where we found that the median number of identities stolen in a data breach is up over last year. This trend has continued since then, with the median now up to 8,404 identities per breach. (Note that this is the median number rather than an average. When looking at data like this, the average can be misleading since a few large data breaches can cause a huge increase.)

For this month, let's take a closer look at the types of information being stolen during data breaches and what can be done with that information. We've broken down the top ten information types that are reported as stolen in data breaches by how often they appear in breaches as a whole.

To do this, we took a look at more of the data gathered through our Norton Cybercrime Index. The data breach section of the Norton CCI is derived from data breaches that have been reported by legitimate media sources and have exposed personal information. Using publicly available data the Norton CCI determines the sectors that were most often affected by data breaches, as well as the most common causes of data loss.

We gathered data on breaches that have occurred so far in 2012 and organized them by the types of information included in the breach. We then organized each type as a percentage of overall breaches, ultimately showing how often the information was exposed across all breaches.

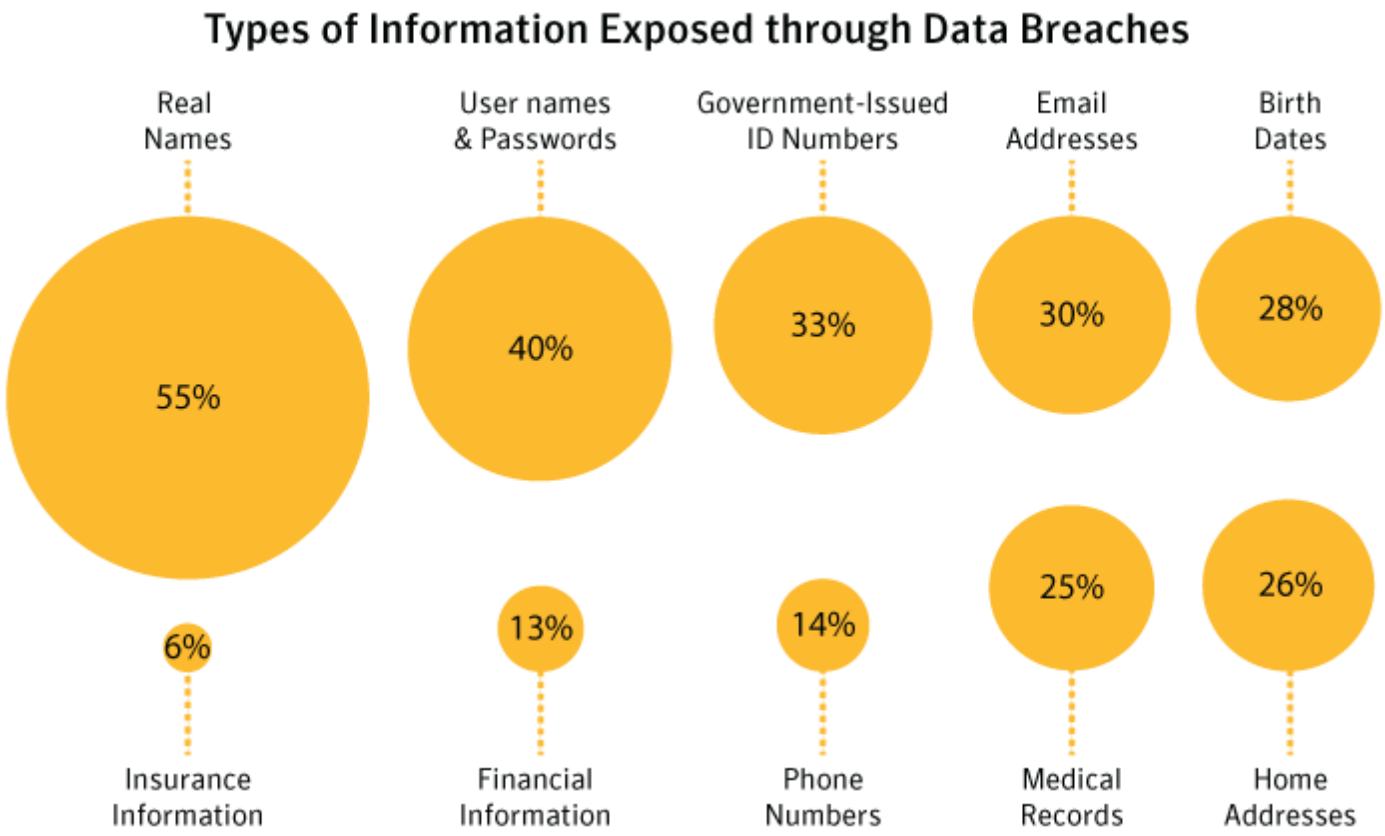


Figure 1 – Percentages of data type exposed in a typical data breach

At first glance, what may seem surprising is that a person's real name is by far the most common item to be stolen in a data breach, where it is obtained 55% of the time. This surpasses even usernames and passwords, most commonly used for online identities, which appears within 40% of all data breaches. This points to a trend where hackers are targeting locations people go to complete tasks, in contrast to years past where breaches may have occurred with

more frequency through message boards or online games. These former hot-spots would have been less likely to include a user's real name, often only requiring an alias for a user name.

In contrast, more than 80% of data breaches that are occurring this year are with organizations whose Internet presence is secondary to their main business, such as the healthcare and education sectors, where online access to services is often set up as a means of convenience instead of a business front. Viewing a website as an auxiliary service may mean laxer security, making them easier targets for data breaches.

What is concerning is that government-issued ID numbers, such as Social Security numbers, are still stolen in so many data breaches. While storing this information would make sense for some sectors such as accounting or healthcare, where knowing such numbers is a necessity, in many cases these numbers are being stolen from organizations that really have no direct need of it. It may be time for consumers, when asked to provide a Social Security number, to being asking the organization just why they need it, and if an alternate identifying number can be provided instead.

What appears to be a silver lining in this analysis is that financial information—such as banking details, credit card details, and salary information—only appears in 13% of all data breaches. This could be due to heavier restrictions on how financial information must be gathered, confirmed, and stored.

What's important to note is that this data does not account for actual cases of identity theft; the data has been stolen, but not necessarily used maliciously. Rather it opens the door for someone with malicious intention to use the information for illicit activities.

A hacker may use some of the information they've gathered in a breach to gather further information. For instance, this information could be used to "confirm" someone's identity over the phone, thus gaining access to further data. In these cases, the hacker is able to work his or her way up the "data chain" in the hopes of obtaining more valuable information.

Most cases of pure monetary theft, where an identity is falsified to purchase goods or services, are done on a much more covert process than buying items with abandon. For example, a thief who has obtained a cache of sensitive data might take one credit card from a list that's been stolen and then test to see if it usable by making a very small purchase—one that would draw little attention on a credit card statement. If the transaction was successful, he or she might sell the credit card details on to another party.

Finally, an attacker could use this information to create fake accounts in someone's name. This could mean misrepresenting someone online, such as in social networking environments. In more extreme cases, the data could be used to blatantly impersonate the individual. While the latter is much rarer, there have been instances of people opening credit cards in other people's names, or impersonating another individual to receive medical treatment.

Overall, it doesn't appear that the rise in identities exposed through data breaches is going to be slowing down any time soon. Fortunately, while not always required by law, it appears to becoming standard practice for organizations that are breached to provide credit monitoring services. The best thing you can do as a consumer is to only provide personal details when absolutely necessary, and keep a close eye on your personal information as much as possible.

Spam: A holiday tradition

with contributions by Nicholas Johnston

It's almost becoming a holiday tradition, though not in the sense of decorating the tree or drinking eggnog. We're all used to being bombarded with holiday advertisements, enticing us to buy goods from various retailers, but what's also becoming the norm is the annual run of holiday spam.

Looking at this year's trends, naturally we see increases in Subject lines targeting certain themes during the lead-up to various days in the holiday period. Take a look at these subject snapshots from the month of November:

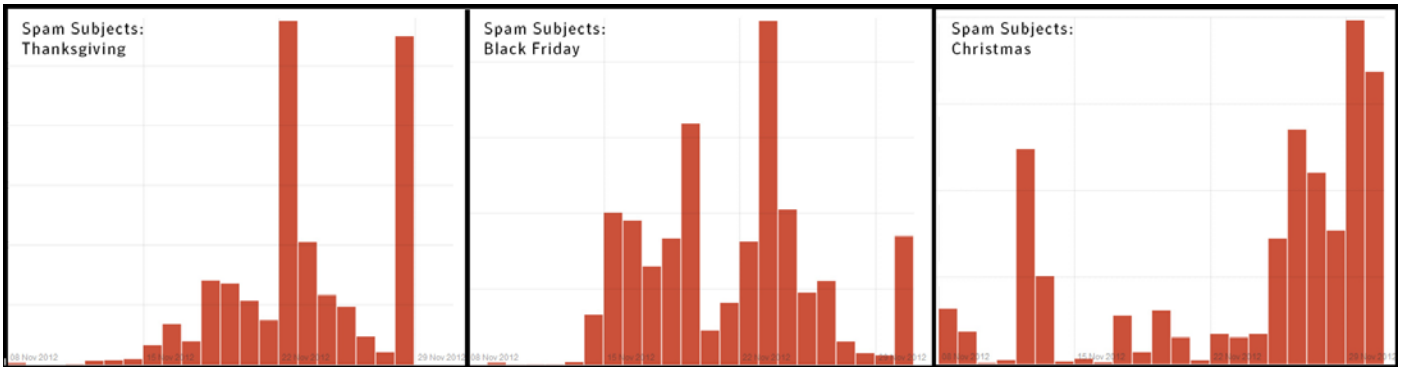


Figure 2 – Spam rates for holiday subject lines

However, the spam messages appear to appeal more to the holiday season in keywords than they do in the body of the message:

Subject:
`Christmas sales`

Message body:

```
Goog morning, dear [REMOVED]!
Huge discount

Exhausted? No desire? Viagra will help! Buy here!

-> Propceia - 0.23$
-- Levtira - 1.84$
-> Cialis - 1.81$
++ Vigara - 0.79$

Take care of your body and it will take care of you. Use our autumn discounts!
```

Some of the websites that these spam messages lead to appear to pay a little more attention to the details of the season however, with banners that fit the holiday spirit. Sometimes getting a full year's jump on early shopping! (Note the "Christmas 2013" mention.)

Figure 3 – Holiday pharmacy spam

Now while many people are around the world are preparing for Christmas, some 419 or advance fee fraud spammers have reminded us that there are plenty of people who don't celebrate Christmas, and plenty of cultural differences which scammers can exploit. We recently saw a fake lottery 419 or advance fee fraud message stating:

```
Your Email Id has Won a whooping sum of four crores eighty lakhs,in Punjab draw please
provide Your Name,Address.
```

It is interesting to see scammers tailoring their mails for the Indian subcontinent by using the South Asian numbering system. A "crore" is ten million and a "lakh" is one hundred thousand. 419 scammers never cease to amaze with their constant tailoring and adaptation.

Finally, we have seen an increase in spam messages with file sizes 10kb or larger. These bigger emails are up 21 percent, from 17.3 percent in October to 38.3 percent of all spam email in November. While our first thoughts were that this could be the result of an increase in image spam, with emails designed to appeal to holiday shoppers, we found that the increases could be attributed to a malware run during the month.

That’s not to say we won’t see an increase in image spam as Christmas approaches. In fact we expect to see the frequency of large spam emails to stay up, if not increase in December. In much the same way that retailers send out larger catalogs around the holidays seasons, spammers will likely send out larger spam messages, hoping to cash in on the holiday season.

Global Trends & Content Analysis

Symantec has established some of the most comprehensive sources of Internet threat data in the world through the Symantec™ Global Intelligence Network, which is made up of more than 64.6 million attack sensors and records thousands of events per second. This network monitors attack activity in more than 200 countries and territories through a combination of Symantec products and services such as Symantec DeepSight™ Threat Management System, Symantec™ Managed Security Services and Norton™ consumer products, and other third-party data sources.

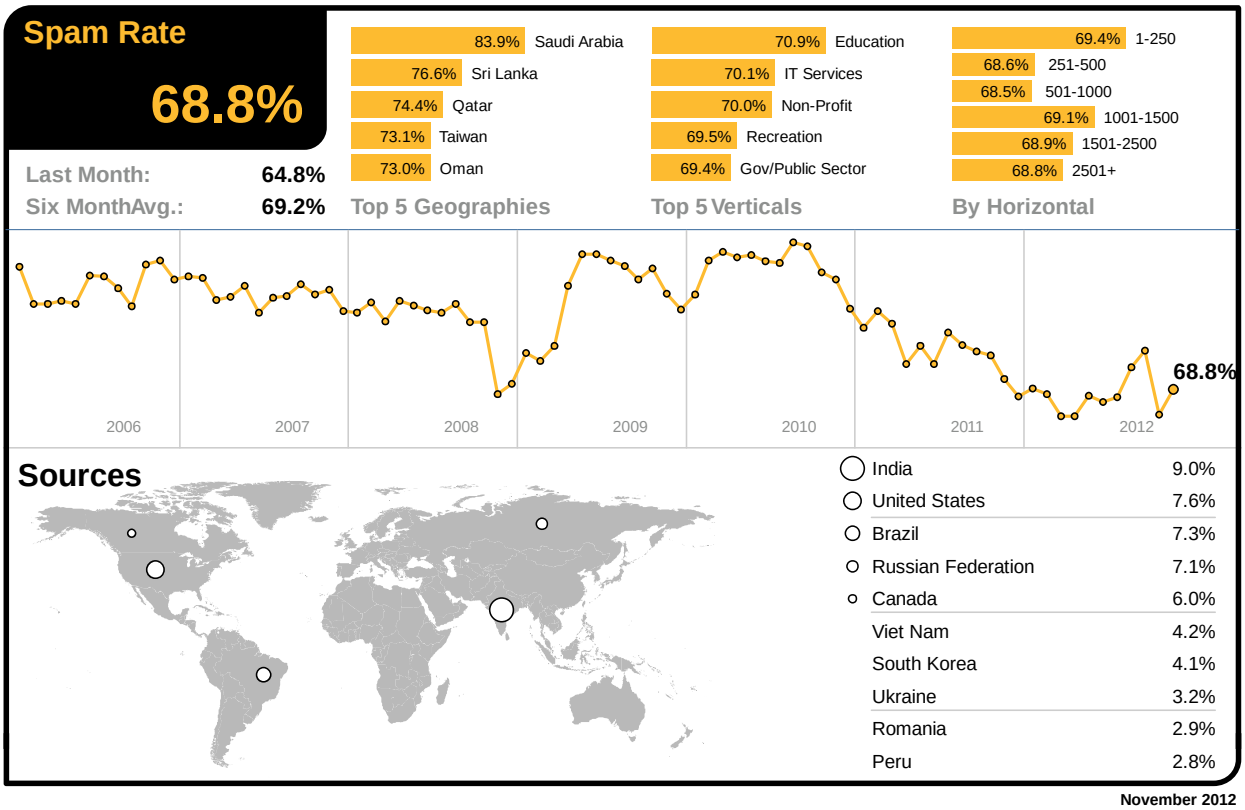
In addition, Symantec maintains one of the world's most comprehensive vulnerability databases, currently consisting of more than 47,662 recorded vulnerabilities (spanning more than two decades) from over 15,967 vendors representing over 40,006 products.

Spam, phishing and malware data is captured through a variety of sources, including the Symantec Probe Network, a system of more than 5 million decoy accounts; Symantec.cloud and a number of other Symantec security technologies. Skeptic™, the Symantec.cloud proprietary heuristic technology is able to detect new and sophisticated targeted threats before reaching customers' networks. Over 8 billion email messages and more than 1.4 billion Web requests are processed each day across 15 data centers. Symantec also gathers phishing information through an extensive antifraud community of enterprises, security vendors, and more than 50 million consumers.

These resources give Symantec's analysts unparalleled sources of data with which to identify, analyze, and provide informed commentary on emerging trends in attacks, malicious code activity, phishing, and spam. The result is the annual Symantec Internet Security Threat Report, which gives enterprises and consumers the essential information to secure their systems effectively now and into the future.

Spam Analysis

In November, the global ratio of spam in email traffic rose by 4.0 percentage point since October, to 68.8 percent (1 in 1.45 emails). This follows the continuing trend of global spam levels diminishing gradually since the latter part of 2011.



November 2012

Global Spam Categories

The most common category of spam in November is related to the Sex/Dating category, with 57.72 percent.

Category Name	November 2012	October 2012
Sex/Dating	57.72%	62.73%
Pharma	14.71%	9.79%
Watches	12.69%	3.74%
Jobs	5.46%	10.45%
Mobile	3.77%	0.19%
Software	3.38%	2.49%
Casino	1.23%	0.75%
419/scam/lotto	0.20%	0.11%
Newsletters	0.08%	0.04%
Degrees	0.01%	0.35%

Spam URL Distribution based on Top Level Domain Name

The proportion of spam exploiting URLs in the .com top-level domain increased in November, as highlighted in the table below. This is in line with a slight increase in .com top-level domains this month.

TLD	November 2012	October 2012
.com	64.1 %	63.1 %
.net	6.5 %	6.8 %
.ru	6.2 %	6.2 %
.org	3.3 %	n/a

Average Spam Message Size

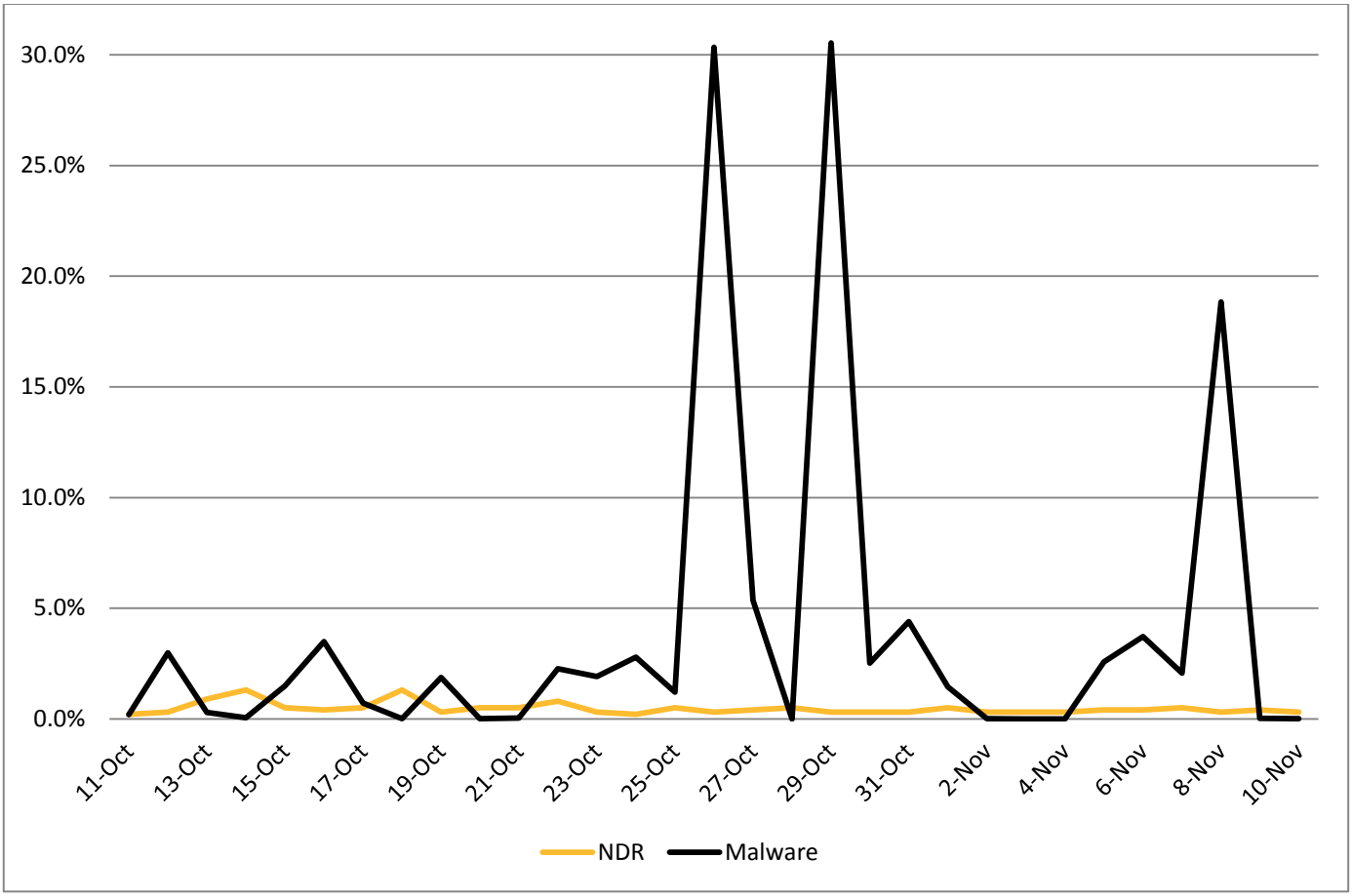
In November, the proportion of spam emails that were 5Kb in size or less decreased by 5.0 percentage points. Furthermore, the proportion of spam messages that were greater than 10Kb in size increased by 21 percent, as can be seen in the following table.

Message Size	November 2012	October 2012
0Kb – 5Kb	36.8 %	41.8 %
5Kb – 10Kb	24.9 %	40.9 %
>10Kb	38.3 %	17.3 %

Spam Attack Vectors

November highlights the decrease in spam emails resulting in NDRs (spam related non-delivery reports). In these cases, the recipient email addresses are invalid or bounced by their service provider. The proportion of spam that contained a malicious attachment or link increased, with periodic spikes of spam activity during the period, as shown in the chart below.

Symantec™

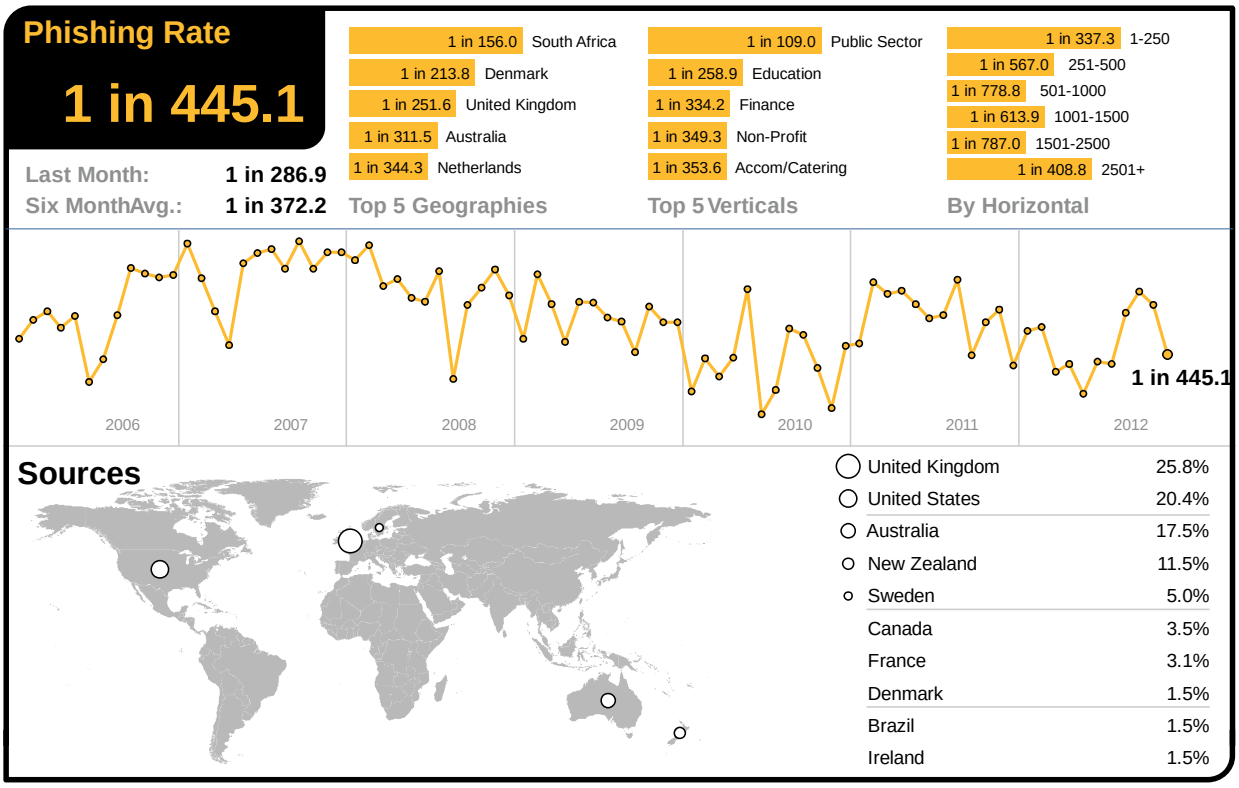


NDR spam, as shown in the chart above, is often as a result of widespread dictionary attacks during spam campaigns, where spammers make use of databases containing first and last names and combine them to generate random email addresses. A higher-level of activity is indicative of spammers that are seeking to build their distribution lists by ignoring the invalid recipient emails in the bounce-backs. The list can then be used for more targeted spam attacks containing malicious attachments or links. This might indicate a pattern followed by spammers in harvesting the email addresses for some months and using those addresses for targeted attacks in other months.

Symantec™

Phishing Analysis

In November, the global phishing rate decreased by 0.124 percentage points, taking the global average rate to one in 445.1 emails (0.225 percent) that comprised some form of phishing attack.



November 2012

Analysis of Phishing Websites

The overall phishing increased by about 8.5 percent this month. Unique domains decreased by about 14 percent as compared to the previous month. Phishing websites that used automated toolkits increased by 37 percent. Phishing websites with IP domains (for e.g. domains like http://255.255.255.255) decreased by about 19 percent. Webhosting services comprised of 2 percent of all phishing, a decrease of 29 percent from the previous month. The number of non-English phishing sites decreased by 8 percent. Among non-English phishing sites, French, Italian, Portuguese, and Chinese were highest in October.

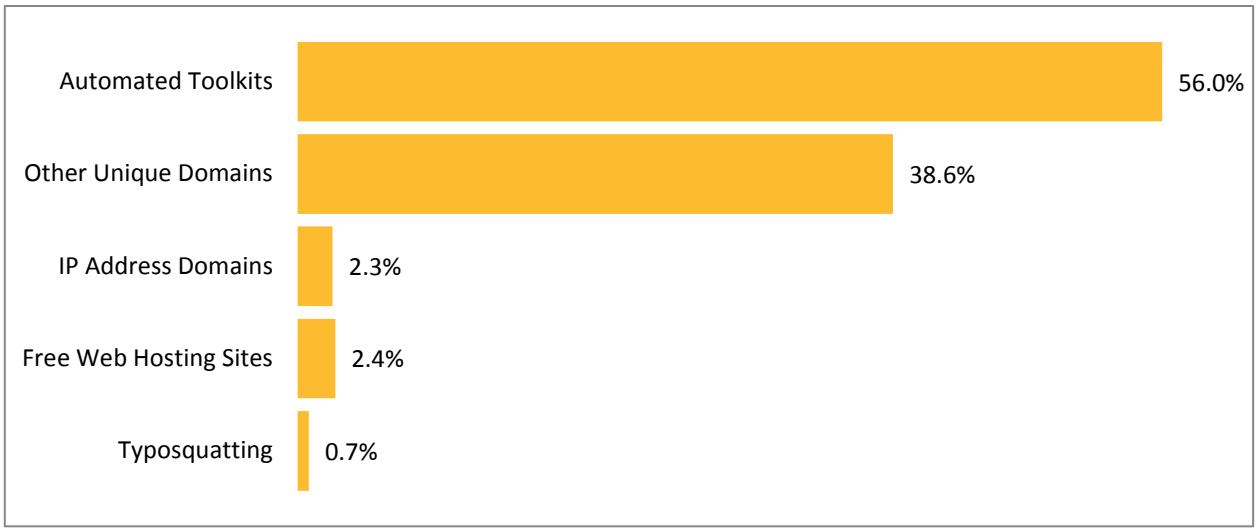
Geographic Location of Phishing Websites

Country	October*	September
United States	54.7%	54.2%
Germany	4.8%	5.0%
United Kingdom	3.6%	3.8%
Canada	3.4%	3.4%
China	3.1%	2.1%
Brazil	2.9%	3.0%
France	2.5%	2.7%
Russia	2.1%	2.0%
Netherlands	2.0%	2.4%
Turkey	1.3%	1.3%

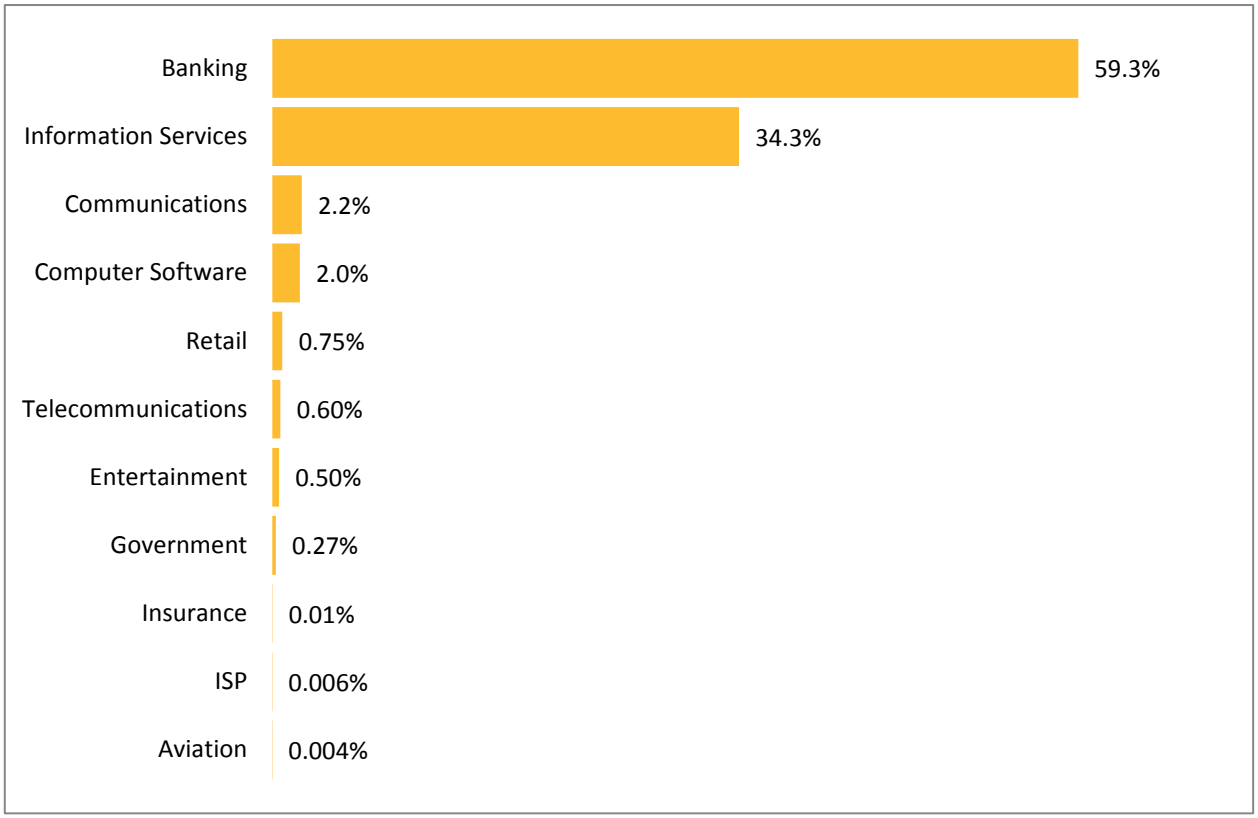
November 2012

Symantec™

Tactics of Phishing Distribution



Organizations Spoofed in Phishing Attacks, by Industry



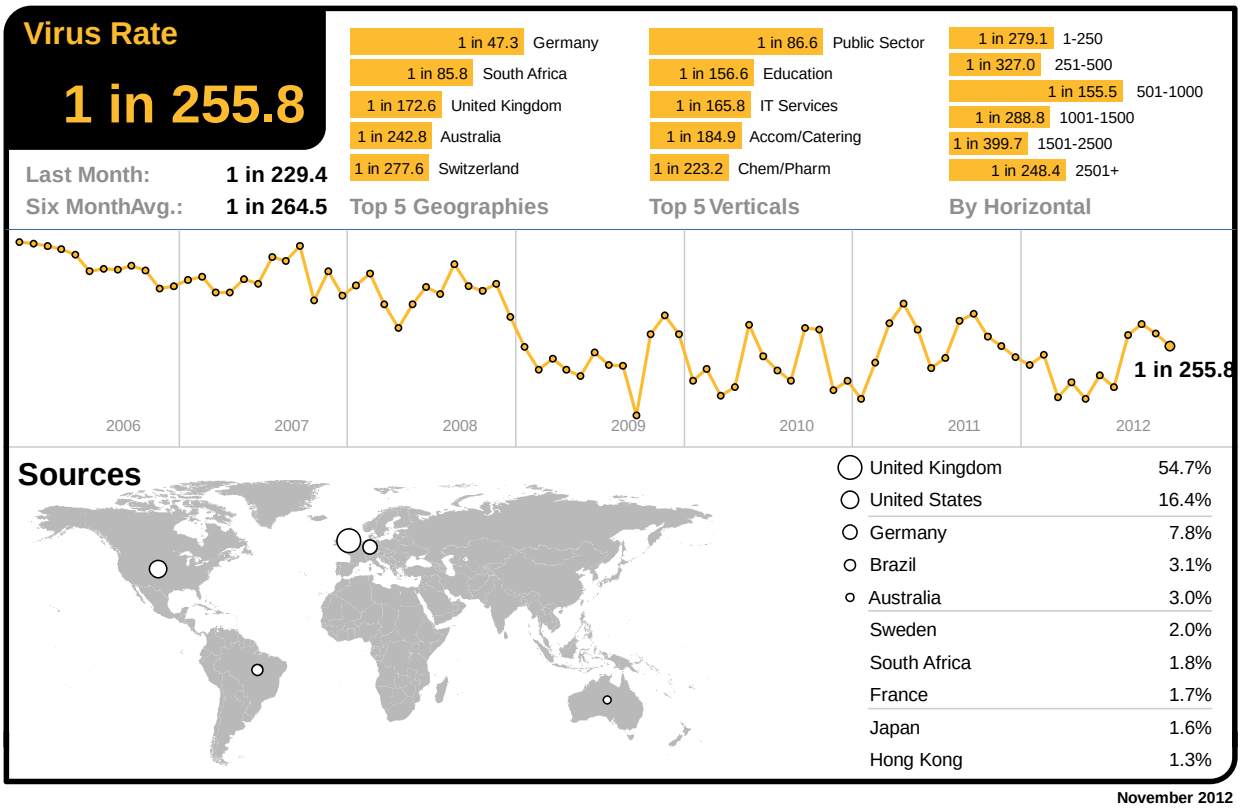
Symantec™

Malware Analysis

Email-borne Threats

The global ratio of email-borne viruses in email traffic was one in 255.8 emails (0.391 percent) in November, a decrease of 0.05 percentage points since October.

In November, 13.0 percent of email-borne malware contained links to malicious websites, 10.6 percentage points lower than October.



November 2012

Frequently Blocked Email-borne Malware

The table below shows the most frequently blocked email-borne malware for November, many of which relate to generic variants of malicious attachments and malicious hyperlinks distributed in emails. Approximately 35.4 percent of all email-borne malware was identified and blocked using generic detection.

Malware identified generically as aggressive strains of polymorphic malware accounted for 15.2 percent of all email-borne malware blocked in November.

Malware Name	% Malware
Suspicious.JIT.a-SH	15.42%
Suspicious.JIT.a.dam	6.74%
W32/Generic.dam	6.24%
W32/Bredolab.gen!eml.k-SH	5.85%
Exploit/Link-generic-ee68	5.44%
W32/Bredolab.gen!eml.j-SH	5.16%
Trojan.Sasfis.dam	3.68%
EML/Worm.XX.dam	2.99%
Link-Trojan.Blackhole.I	2.62%
W32/Bredolab.gen!eml.j	1.77%

The top-ten list of most frequently blocked malware accounted for approximately 15.8 percent of all email-borne malware blocked in November.

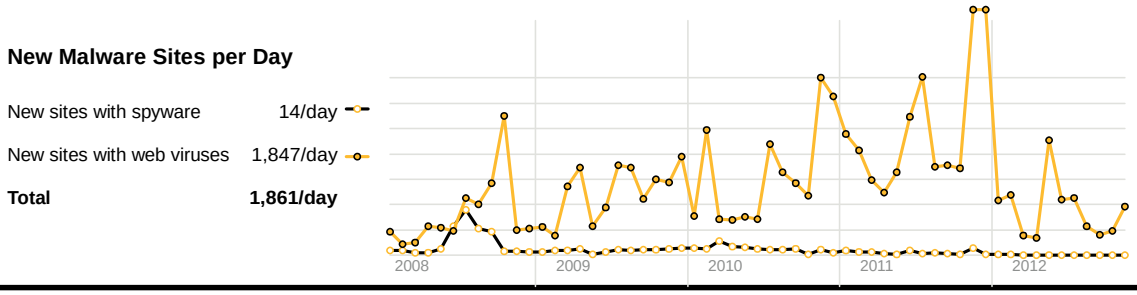
Symantec™

Web-based Malware Threats

In November, Symantec Intelligence identified an average of 1,847 websites each day harboring malware and other potentially unwanted programs including spyware and adware; an increase of 97.9 percent since October. This reflects the rate at which websites are being compromised or created for the purpose of spreading malicious content. Often this number is higher when Web-based malware is in circulation for a longer period of time to widen its potential spread and increase its longevity.

As detection for Web-based malware increases, the number of new websites blocked decreases and the proportion of new malware begins to rise, but initially on fewer websites. Further analysis reveals that 33.3 percent of all malicious domains blocked were new in November; a decrease of 5.2 percentage points compared with October. Additionally, 11.0 percent of all Web-based malware blocked was new in November; a decrease of 0.01 percentage points since October.

Web Security Services Activity:



The chart above shows the increase in the number of new spyware and adware websites blocked each day on average during November compared with the equivalent number of Web-based malware websites blocked each day.

Web Policy Risks from Inappropriate Use

Some of the most common triggers for policy-based filtering applied by Symantec Web Security.cloud for its business clients are social networking, advertisements and pop-ups, and streaming media category. Many organizations allow access to social networking websites, but facilitate access logging so that usage patterns can be tracked and in some cases implement policies to only permit access at certain times of the day and block access at all other times. Web-based advertisements pose a potential risk though the use of “malvertisements,” or malicious advertisements. These may occur as the result of a legitimate online ad-provider being compromised and a banner ad being used to serve malware on an otherwise harmless website. Streaming media is increasingly popular when there are major sporting events or high profile international news stories. This activity often results in an increased number of blocks, as businesses seek to preserve valuable bandwidth for other purposes.

Web Security Services Activity:

Policy-Based Filtering		Web Viruses and Trojans		Potentially Unwanted Programs	
Advertisement and Popups	28.9%	JS:Trojan.Script.EY	35.5%	Dropped:Adware.Generic.262597	83.5%
Social Networking	28.9%	Trojan.JS.Agent.HHY	7.6%	Application.DirectDownloade r.A	7.9%
Streaming Media	7.5%	Downloader	5.6%	Spyware.PCAcme	3.6%
Peer-To-Peer	4.2%	JS:Trojan.Iframe.S	5.1%	Application:Android/Counterclank. A	0.4%
Computing and Internet	3.9%	JS:Trojan.Iframe.AXP	2.6%	Adware:Android/AirPush. A	0.4%
Chat	3.0%	Trojan.JS.Agent.GHF	2.0%	Adware.Generic.279017	0.4%
Gambling	2.3%	Trojan.JS.Iframe.BRV	1.4%	Adware:W32/Baidu.gen!B	0.3%
Hosting Sites	2.2%	Trojan.Script.WO	1.4%	Gen:Application.Heur.cmKfbiBPZXoO	0.2%
Games	2.0%	Trojan.JS.Iframe.CFJ	1.2%	Spyware.Ardakey	0.2%
News	1.6%	Gen:Variant.Symmi.2895	1.2%	Adware.Generic.249333	0.2%

November 2012

Endpoint Security Threats

The endpoint is often the last line of defense and analysis; however, the endpoint can often be the first-line of defense against attacks that spread using USB storage devices and insecure network connections. The threats found here can shed light on the wider nature of threats confronting businesses, especially from blended attacks and threats facing

mobile workers. Attacks reaching the endpoint are likely to have already circumvented other layers of protection that may already be deployed, such as gateway filtering.

The table below shows the malware most frequently blocked targeting endpoint devices for the last month. This includes data from endpoint devices protected by Symantec technology around the world, including data from clients which may not be using other layers of protection, such as Symantec Web Security.cloud or Symantec Email AntiVirus.cloud.

Malware Name[1]	% Malware
W32.Sality.AE	6.52%
W32.Ramnit!html	6.01%
W32.Downadup.B	4.91%
W32.Ramnit.B	4.86%
W32.Ramnit.B!inf	3.89%
W32.Almanahe.B!inf	2.35%
W32.Virut.CF	2.09%
W32.SillyFDC.BDP!lnk	1.85%
W32.Xpaj.B	1.06%
W32.Virut!html	1.01%

For much of 2012, variants of W32.Sality.AE[2] and W32.Ramnit[3] had been the most prevalent malicious threats blocked at the endpoint. Variants of W32.Ramnit accounted for approximately 15.0% of all malware blocked at the endpoint in November, compared with 7.2 percent for all variants of W32.Sality.

Approximately 10.2 percent of the most frequently blocked malware last month was identified and blocked using generic detection. Many new viruses and Trojans are based on earlier versions, where code has been copied or altered to create a new strain, or variant. Often these variants are created using toolkits and hundreds of thousands of variants can be created from the same piece of malware. This has become a popular tactic to evade signature-based detection, as each variant would traditionally need its own signature to be correctly identified and blocked.

By deploying techniques, such as heuristic analysis and generic detection, it's possible to correctly identify and block several variants of the same malware families, as well as identify new forms of malicious code that seek to exploit certain vulnerabilities that can be identified generically.

[1] *For further information on these threats, please visit: http://www.symantec.com/business/security_response/landing/threats.jsp*
[2] *http://www.symantec.com/security_response/writeup.jsp?docid=2006-011714-3948-99*
[3] *http://www.symantec.com/security_response/writeup.jsp?docid=2010-011922-2056-99*

About Symantec Intelligence

Symantec Intelligence is a respected source of data and analysis for messaging security issues, trends and statistics. Symantec.cloud Intelligence publishes a range of information on global security threats based on data captured through a variety of sources, including the Symantec Global Intelligence Network, the Symantec Probe Network (a system of more than 5 million decoy accounts), Symantec.cloud and a number of other Symantec security technologies. Skeptic™, the Symantec.cloud proprietary technology uses predictive analysis to detect new and sophisticated targeted threats, protecting more than 11 million end users at more than 55,000 organizations ranging from small businesses to the Fortune 500.

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. More information is available at www.symantec.com.

Copyright © 2012 Symantec Corporation. All Rights Reserved.

Symantec, the Symantec Logo, and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the US and other countries. Other names may be trademarks of their respective owners.

NO WARRANTY. The information contained in this report is being delivered to you AS-IS, and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the information contained herein is at the risk of the user. This report may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice. No part of this publication may be copied without the express written permission of Symantec Corporation, 350 Ellis Street, Mountain View, CA 94043.