Global spam landscape: Snowshoe spam

Version 1.0: November 26, 2014
Analyst: *Francisco Pardo*

Executive summary

The dictionary defines a snowshoe as: *A racket-shaped frame containing interlaced strips, as of leather, that can be attached to the foot to facilitate walking on deep snow.*

Wisegeek.com has a very good, concise explanation of the reason behind the name, snowshoe, being applied to a certain spamming technique*:*

"The snowshoe is actually an excellent analogy to describe this spamming technique. Snowshoes are designed to spread a large weight across a wide area so that the wearer does not break through crusts of snow and ice, and snowshoe spamming distributes a broad load of spam across a varied array of IP addresses in much the same way. Like all spammers, snowshoe spammers anticipate that some of their unwanted emails will be trapped by spam filters. Snowshoe spamming gives more email a chance at getting through to an inbox, where it can reach a computer user."

In 2014, particularly in the middle of the year, Symantec observed an overall increase in what is commonly known as Snowshoe spam. As the explanation we just mentioned implies, this spam technique is known to exploit antispam products' spam definition propagation latency and reliance on IP address reputation by sending large volumes of spam messages in short bursts, which quickly rotate domains and send IP address hops within certain /24 ranges.

This document outlines the variations to Snowshoe patterns Symantec has seen over time and the challenges that arise when it comes to blocking spam that uses this technique.

Snowshoe changes

Spam has always been a business, albeit an underground and illegal business in most countries. Over the last few years, spam messages have become much more similar in style to email marketing and third-party mailer messages. In an attempt to improve the message deliverability of their emails, spammers are increasingly leveraging the Snowshoe technique which, similar to email marketing campaigns, centers on promoting a product or service. And in keeping with the marketing analogy, for those messages that make it into the end-user's inbox, the spammers' next objective is to catch the end-user's eye and get them to open the email, read it, and potentially even click on the included link, or buy the service or product being promoted.

Some spammers even try to create seemingly legitimate brands for their mailing activities, by setting up fake companies (as we have blogged about in the past). Through these fake companies a large amount of domains are registered to be used in spam campaigns. Some of these fake companies will even keep a network-traffic profile similar to that of a legitimate business, primarily sending out spam during a specific timezone's business hours with little or none being sent out at weekends. All this is done in an effort to not raise any red flags, but once the flag is raised and they see their traffic being blocked, the spammers are ready to dump that identity and move onto the next.

Antispam technologies are constantly evolving to combat these spam threats. Newly observed email header and body patterns, as well as information about where these messages originate from is used by antispam technology to force the spammers to find different ways to try to keep ahead in the endless cat-and-mouse game. After all, the spammers' profits and business model are tied to how many messages they can deliver to the user's inbox without getting blocked by antispam measures.

Snowshoe campaigns commonly have the following characteristics:

- Originate from IP address ranges with a neutral reputation
- Use a large IP address range to dilute the amount of spam sent from each IP address
- Contain features (such as the subject line, from line, and URLs) which change quickly
- Include the call-to-action in the URL
- Use large quantity of "throw-away" domains in a single spam campaign

However, in the latest Snowshoe campaigns, we have noticed certain shifts from some of the most common characteristics, as previously mentioned, along with other changes:

- IP addresses belong to small blocks of consecutive IP addresses
- IP addresses have fast sent rates, as opposed to previously slower, larger attacks
- Higher rotation rate of email templates, which rarely use the same series of words or images for an extended period of time
- Abuse of many new generic top-level domains (GTLDs). The scammers do this to take advantage of sales promotions for these new domains and to use the domains before they implement a proper abuse infrastructure
- Much higher percentage of the use of anonymous or private domain registry services

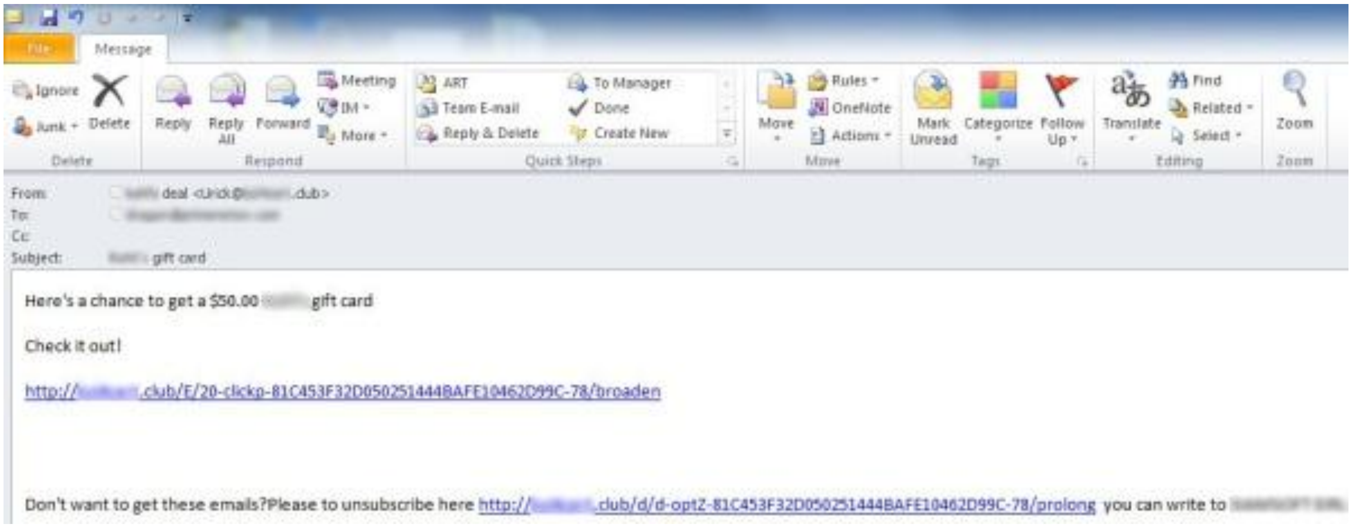
The following are a few samples of the subject headers in these campaigns:

- 2014 Models Overstocked (Ride for half)
- Everything below Kelly Blue Book
- Restore your thin hair back to normal
- Select a 2014 (Ford)

- Organic treats food 75% off

The following are a few samples of the email headers included in these messages:

- From: "CarClearanceLot" <CarClearanceLot@[REMOVED].club>
- From: "[REMOVED] Wholesale-Bonus" <Mackenzie@[REMOVED].com>
- From: "CarSavingsEvents" <CarSavingsEvents@[REMOVED].club>
- From: "All 2014 Autos Below KBB" <Tessa_Nash@[REMOVED].com>
- From: "PriceNewCar" <PriceNewCar@[REMOVED].club>
- From: "[REMOVED] Shopper Rewards" <Makayla@[REMOVED].xyz>
- From: Gift Cards <party@[REMOVED].website>



From: [redacted] deal <cLrick@[redacted].club>
To: [redacted]
Cc:
Subject: [redacted] gift card

Here's a chance to get a $50.00 [redacted] gift card

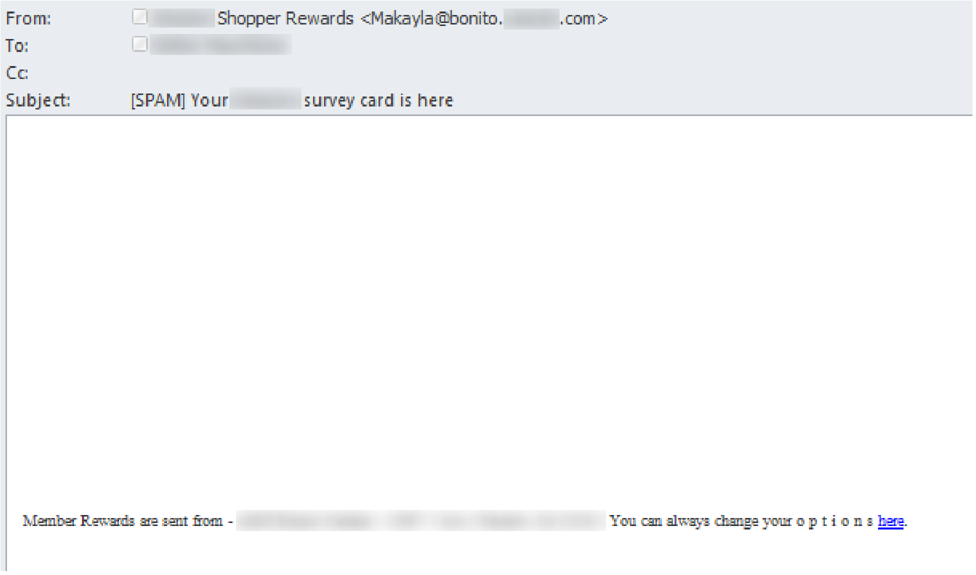
Check it out!

http://[redacted].club/E/20-clickp-81C453F32D050251444BAFE10462D99C-78/broaden

Don't want to get these emails?Please to unsubscribe here http://[redacted].club/d/d-optZ-81C453F32D050251444BAFE10462D99C-78/prolong you can write to [redacted]

Figure 1. Snoeshow-type spam campaign offering a gift card

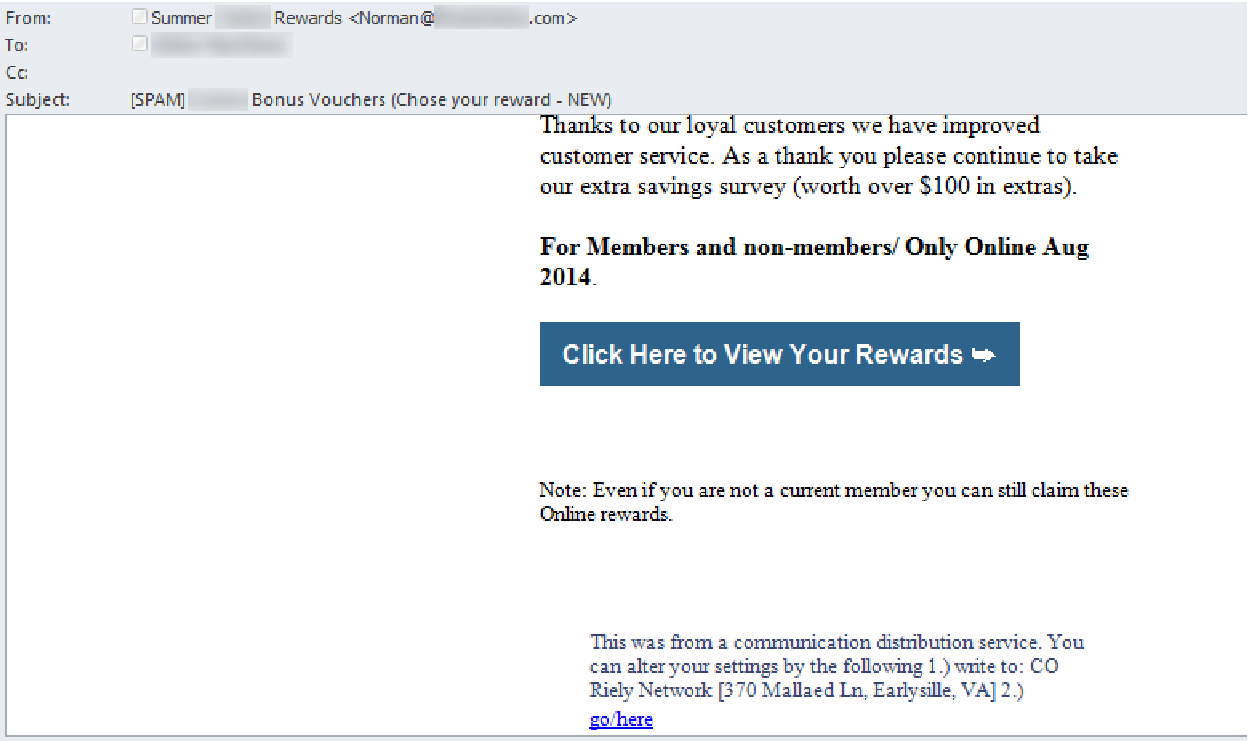
Snoeshoe spam campaigns also attempt to imitate both the look and feel of email marketing messages, such as how the messages are composed. They may even include unsubscribe links and headers in another attempt to avoid being flagged by antispam products and to make the message seem more legitimate.



From: □ [redacted] Shopper Rewards <Makayla@bonito.[redacted].com>
To: □ [redacted]
Cc:
Subject: [SPAM] Your [redacted] survey card is here

Member Rewards are sent from - [redacted] You can always change your options here.

Figure 2. Sample of Snowshoe spam with unsubscribe link



From: □ Summer [redacted] Rewards <Norman@[redacted].com>
To: □ [redacted]
Cc:
Subject: [SPAM] [redacted] Bonus Vouchers (Chose your reward - NEW)

Thanks to our loyal customers we have improved customer service. As a thank you please continue to take our extra savings survey (worth over $100 in extras).

For Members and non-members/ Only Online Aug 2014.

Note: Even if you are not a current member you can still claim these Online rewards.

This was from a communication distribution service. You can alter your settings by the following 1.) write to: CO Riely Network [370 Mallaed Ln, Earlysille, VA] 2.) go/here

Figure 3. Sample of Snowshoe spam with email marketing-style formatting and unsubscribe link

Due to the nature of the Snowshoe technique, the use of IP address reputation-based detection alone is less effective against Snowshoe spam, emphasizing the importance of a multilayered security approach. Symantec works to identify these spammers and adjust or create new filters for these spam campaigns by combining a number of antispam techniques. These methods include using automated analyzers and human analysis on spam messages that are gathered across Symantec's Probe Network or submitted directly from affected customers.

Additional information

- If you have any customers that are continuing to see this type of attack please ensure that they are following configuration best practices and also reporting the samples (with full headers/body intact) following the appropriate stesps
- See the Symantec.cloud Effectiveness User's Guide for anti-spam best practices
    - http://www.symantec.com/docs/TECH222392
- Submit missed spam for analysis, see manually submitting missed spam for customers running Symantec.cloud
    - http://www.symantec.com/docs/TECH222389
- See Symantec Messaging Gateway Best Practices: Spam Control
    - http://www.symantec.com/docs/TECH90043
- Submit missed spam for analysis, see manually submitting missed spam for customers running Symantec's on-prem products
    - http://www.symantec.com/docs/TECH83081

Symantec Message Gateway customers can also leverage Customer Specific Rules, which act as an additional method to filter these messages and, at the same time, provide us with further visibility into the attack.

Further information on global spam statistics can be found on:
http://www.symantec.com/security_response/landing/spam/

Resources

- Snowshoe spam outbreak article: http://www.symantec.com/business/support/index?page=content&id=AL1589
- club gTLD Used in Hit-and-Run Spam Attacks: http://www.symantec.com/connect/blogs/club-gtld-used-hit-and-run-spam-attacks
- Snowshoe Spam--a New Type of Junk Email--Starting to Clog Inboxes: http://www.eweek.com/security/snowshoe-spam-a-new-type-of-junk-email-starting-to-clog-inboxes.html
- What is Snowshoe Spamming: http://www.wisegeek.com/what-is-snowshoe-spamming.htm#didyouknowout
- My (Failed) Visits to Spammer’s Offices: http://www.symantec.com/connect/blogs/my-failed-visits-spammers-offices

About Symantec

Symantec Corporation is an information protection expert that helps people, businesses and governments seeking the freedom to unlock the opportunities technology brings -- anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company, operating one of the largest global data-intelligence networks, has provided leading security, backup and availability solutions for where vital information is stored, accessed and shared. The company's more than 20,000 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2014, it recorded revenues of $6.7 billion. To learn more go to www.symantec.com or connect with Symantec at: go.symantec.com/socialmedia

More information is available at *www.symantec.com*

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527-8000
1 (800) 721-3934
www.symantec.com

Any technical information that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY. The technical information is being delivered to you as is and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained herein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.