proofpoint

# Proofpoint Threat Report

## November 2013

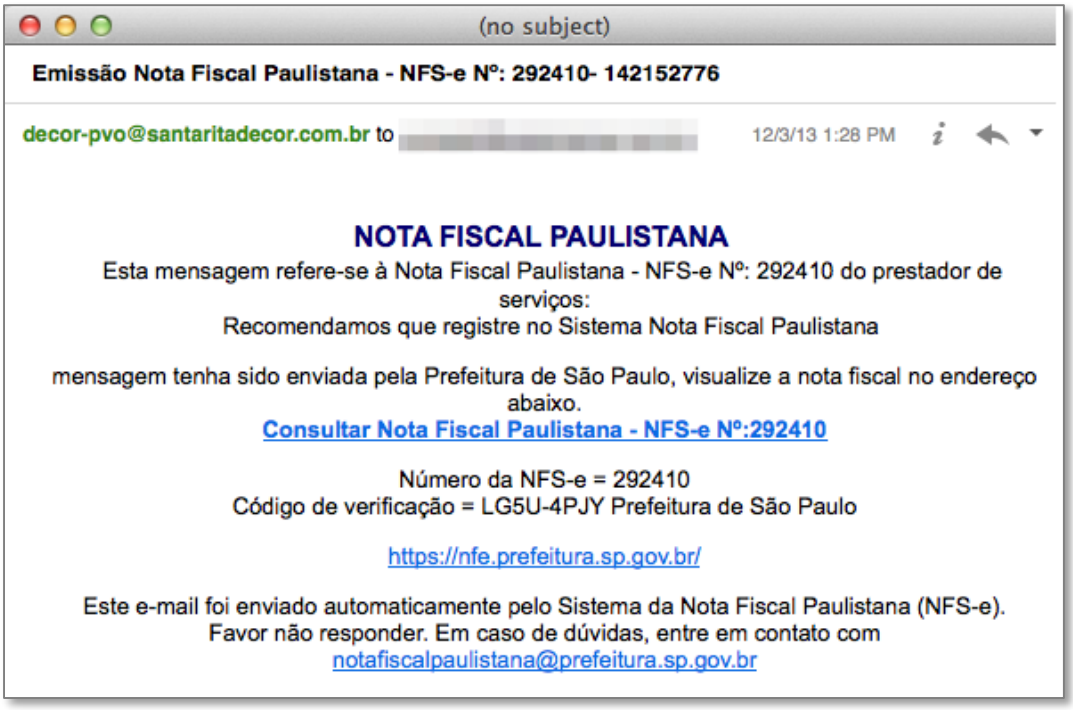
The Proofpoint Threat Report explores threats, trends, and transformations that we see within our customer base and in the wider security marketplace.

### Threat Models

The past four Threat Report editions discussed four major malware attacks; Targeted Attacks, Malvertising, Longlining and Watering Hole Attacks. This month we turn our focus back to specific threat models.

**Hiding Malware Inside SSL**

Attackers have been relying on a number of techniques to infect users. One method is to send links directly to the malware, almost always packed inside a zip file, and convince the user to run the file manually. While this has a lower infection rate than drive-by download attacks, it involves none of the complex infrastructure required for a successful exploit kit campaign. One way attackers are keeping things simple is by using Dropbox to host the malware. With this approach they don't need to setup a website, or bother to compromise a legitimate site. The cloud makes life easier for everyone, including the bad guys. An example campaign, clearly targeting Brazilian users, used this lure:

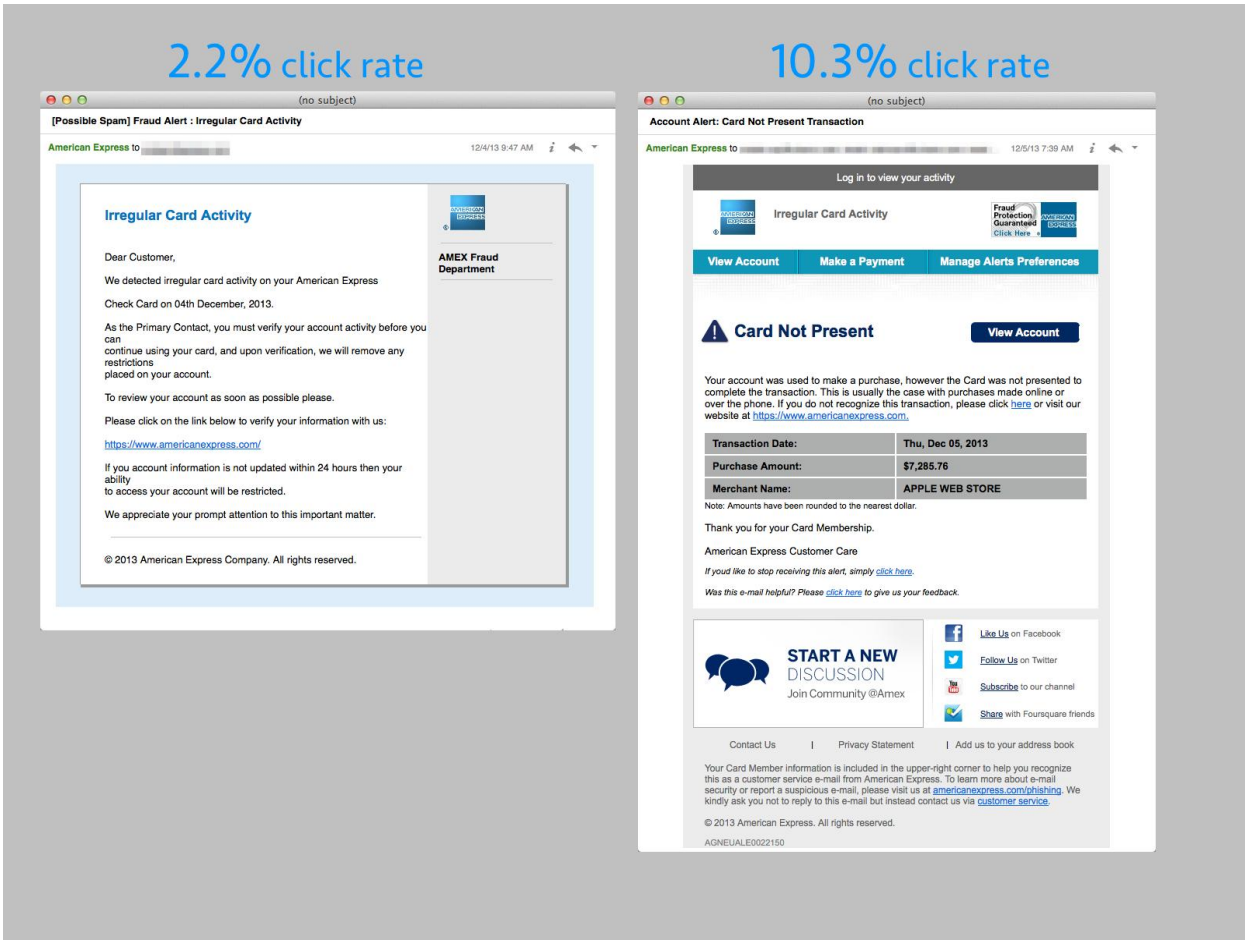



All the links in the email are spoofed, and instead of leading to the legitimate Brazilian government sites, clicks are sent to a Dropbox hosted piece of malware. One of the Dropbox URLs in this case was: https://dl.dropboxusercontent.com/XXXX/XXXXXXXXX/nfe.fazenda.gov.br-N-007.874-12-2013.zip. (Note: The XXXXs are added to de-fang the URL)

What is interesting about this URL is that it uses https:// (SSL) to encrypt the transaction. Some sandboxes are completely blind to this malware, as most cannot decrypt the SSL traffic. This sandbox would only see SSL traffic to Dropbox, which is normal in a modern enterprise. To make things more interesting, the malware in this campaign downloads three (3) additional pieces of malware, all of which are encrypted with some form of custom encryption, further cloaking their presence. Proofpoint's Targeted Attack Protection examines the email message, the application layer, instead of the network traffic and has full visibility. Targeted Attack Protection can detect and stop these types of attacks, protecting your users and company assets.

**Match the Hatch**

Fly fishing aficionados recognize the wisdom in the phrase "Match the Hatch". It refers to matching the fly with the height of an insect hatch, increasing one's catch. In a recent American Express malware campaign, Proofpoint researchers compared two phishing lures on successive days. There was a substantial difference in the number of clicks between the two days. Here are the two templates, along with the percent of messages that were clicked by users:




The second lure clearly "matched the hatch". The result was a 79% higher click rate with the second lure. When comparing the two lures; the large dollar value in bold text, and the increased use of trusted brand logos stand out. It's clear that attackers can dramatically increase the efficacy of a campaign by picking the right "hatch".

## Threat News

### Phishing Emails Using Google Docs Lures

The SANS Institutes ISC (Internet Storm Center) issued a warning on a scam using Google Docs as the phishing bait. The lure email contains a link to a bogus web email provider in what turns out to be a credential phish. Details can be found here: http://www.spamfighter.com/News-18688-ISC-Warns-Phishing-Emails-Abusing-Google-Docs-Circulating-on-Internet.htm

### What Can You Learn from Others Data Breaches?

The inventiveness of attackers is limitless. Keeping systems patched is paramount. It's crucial to minimize public access, via the web, to sensitive databases. Organizations must reconsider the data an endpoint is allowed to store from centralized databases. All are valuable lessons gleaned from four

2013 data breaches highlighted in this Dark Reading article http://www.darkreading.com/database/lessons-learned-from-4-major-data-breach/240164264.

### Commtouch finds 343,972 new malicious websites in November

Proofpoint partner Commtouch, specifically their Security Lab, uncovered 343,972 new malicious websites in November. Details of their findings are enumerated in the following blog post, https://blog.commtouch.com/cafe/miscellaneous/343927-new-malicious-sites-commtouch-security-number-of-the-month-for-november

## Threat Insight Blog

This month we introduce a new section, Threat Insight Blog. Interesting posts from Proofpoint's new threat blog, Threat Insight, will be highlighted. Subscribe to Threat Insight and join the conversation at http://www.proofpoint.com/threatinsight.

### Malware Campaign that Says "Whatsapp" Goes Nuclear

For many weeks now we've been seeing a targeted malware campaign that uses the WhatsApp brand, a mobile instant messaging application, as the lure for its malware campaign. The reason this campaign stood out is due to its use of the Nuclear Exploit Kit, a GeoIP database to do some interesting customizations and some variance in the way the user machine was attacked.

Full post is found here, http://www.proofpoint.com/threatinsight/posts/malware-campaign-that-says-whatsapp-goes-nuclear.php

### Holiday shopping season = more threat campaigns, but will users click?

Some of the most effective malware campaigns we've seen have been those that use eCommerce-related themes such as "order confirmations" or "shipping confirmations" from well-known retailers. Given the holiday season and Christmas shopping, we decided to take a look back at some campaigns we observed in 2013 as we expect the number of these attacks to increase over the next 6 weeks across all regions including North America, Europe, and Asia.

Full details are here, http://www.proofpoint.com/threatinsight/posts/holiday-shopping-season-equal-more-threat-campaigns-but-will-users-click.php

**Healthcare reform also driving up watering hole attacks**

As year-end nears, and Obamacare takes effect, Proofpoint systems have observed a number of compromised websites related to health care topics serving up malware.

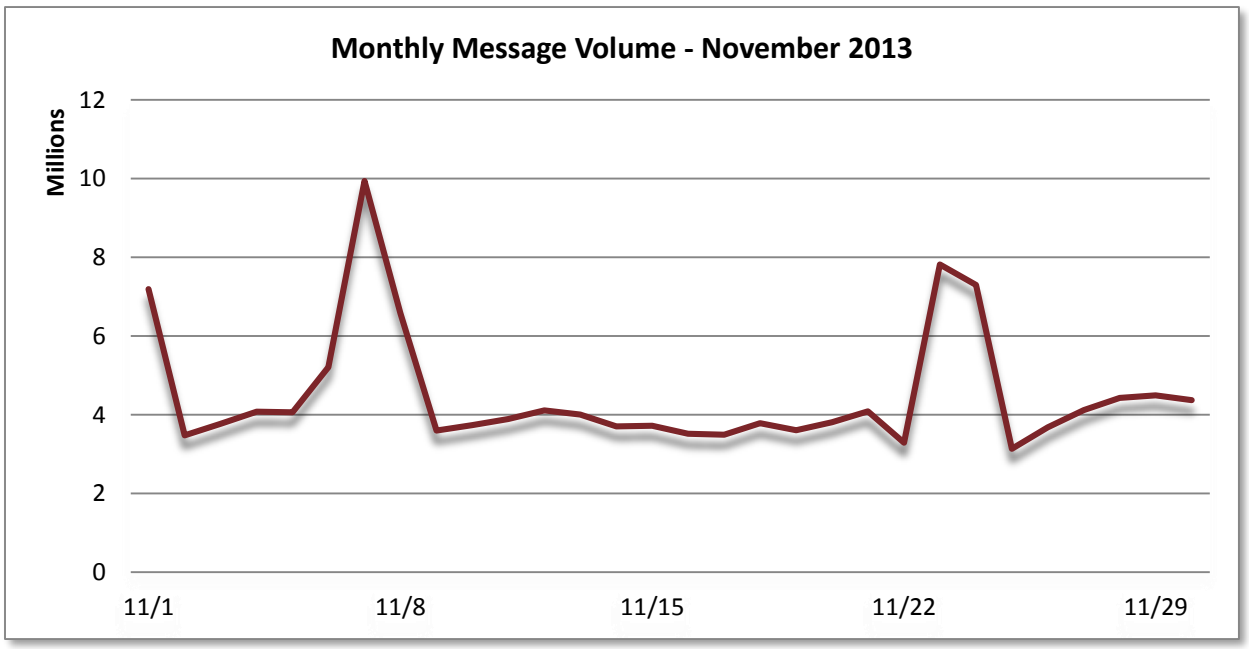
Our research team looked through the last 90 days of all the millions of URLs we have found to be malicious in our sandbox, and extracted the ones that seemed related to healthcare. We then removed the domains that were abused as part of spam campaigns, or were blatant SEO websites, leaving only those we could confirm were serving up malware directly in a watering hole-style attack. We were left with 43 domains, all of which we observed serving up malware in the last 90 days. Websites with domains like "accesshealthsystems.com" and "advancemedicals.com" feature among these.

The full post can be found at, [http://www.proofpoint.com/threatinsight/posts/healthcare-reform-also-driving-up-watering-hole-attacks.php](http://www.proofpoint.com/threatinsight/posts/healthcare-reform-also-driving-up-watering-hole-attacks.php)

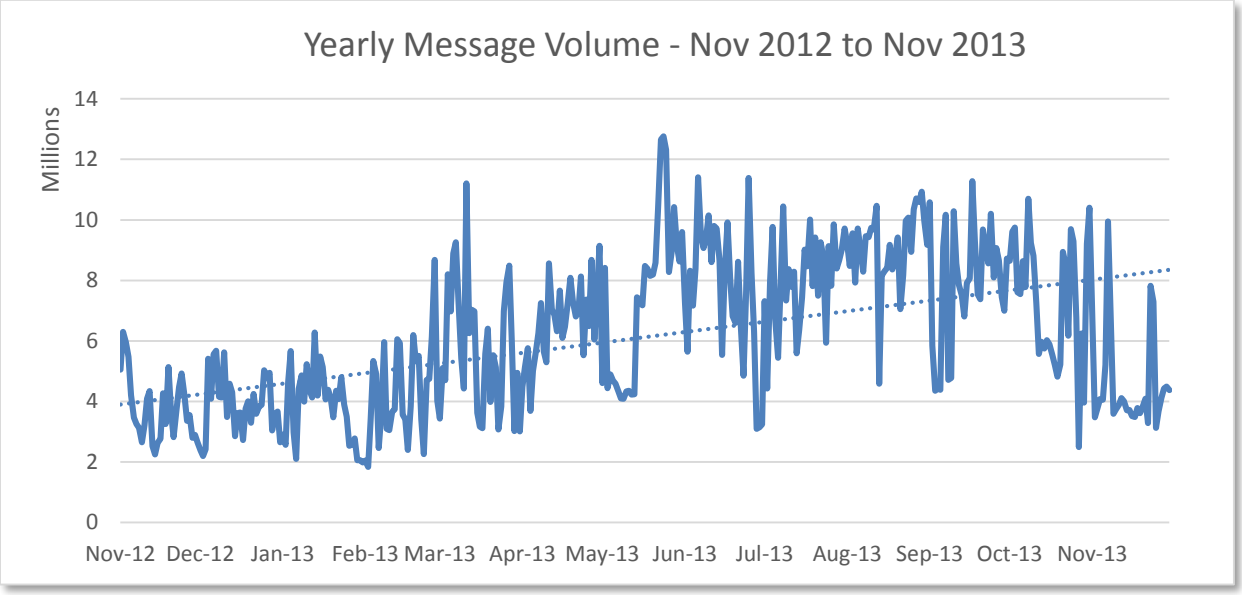
## Threat Trends

### Spam Volume Trends

Proofpoint tracks spam volumes via a system of honeypots. The volumes historically track with that of our customer base. Daily spam volumes dropped significantly from October to November. We again saw volumes across a wide range, from just below 10 million to just above 3 million. Volumes peaked at the beginning of the month but saw a substantial trough during the middle of the month. Additionally, lower day to day spam volumes were experienced in November. For example volumes on October 30 checked in at 9,209,685 compared to November 30 where only 4,373,549 spam messages were recorded, a 52% decrease.



Spam volumes decreased again month over month in November by a substantial 38.17%. A third straight monthly decrease in volumes and a 58.53% decrease over three months. This downward trend has given back most of the previously reported increase. Recall October's spam volumes numbers had increased 47.37% since January. With the latest data the increase is a single digit 6%. Perhaps this portends a larger market shift from standard spam to more lucrative malicious attacks such as long-lining.




### Spam Sources by Country

The Top 5 spam sources shifted in November. The European Union continues to be the number one spam generating region in the world and it was the only consistent rank in November. China jumped to second from fifth. The United States dropped to number three. Japan entered the fray to take fourth, marking the first time Japan has ranked in the top spots. India shifted down to fifth. The following table shows the Top 5 spam sending countries for the last six months.

| | | June '13 | July '13 | August '13 | September '13 | October '13 | November '13 |
|---|---|---|---|---|---|---|---|
| Rank | 1st | European Union (EU) | EU | EU | EU | EU | EU |
| | 2nd | United States (US) | US | US | US | US | China |
| | 3rd | Taiwan | India | Argentina | India | India | US |
| | 4th | Spain | Taiwan | India | Argentina | Argentina | Japan |
| | 5th | China | Argentina | Taiwan | Taiwan | China | India |

The table below details the percentage of total spam volume for each ranking. The European Union recorded a month over month decrease, but continues to generate most of the world's spam. China increased its spam output 300+ percent in November to just over 12% of the recorded volume.

| October 2013 | | | November 2013 | | |
|---|---|---|---|---|---|
| **1** | EU | 18.69% | 1 | EU | 13.97% |
| **2** | USA | 6.68% | **2** | China | 12.22% |
| **3** | India | 4.09% | **3** | US | 7.26% |
| **4** | Argentina | 3.93% | **4** | Japan | 3.37% |
| **5** | China | 3.68% | **5** | India | 3.33% |


For additional insights visit us at
www.proofpoint.com/threatinsight

proofpoint

Proofpoint, Inc.
892 Ross Drive, Sunnyvale, CA 94089
Tel: +1 408 517 4710
www.proofpoint.com