proofpoint

Proofpoint Threat Report

July 2013

The following information explores specific threats, trends, and transformations that Proofpoint is seeing both within the Proofpoint customer base and in the wider marketplace.

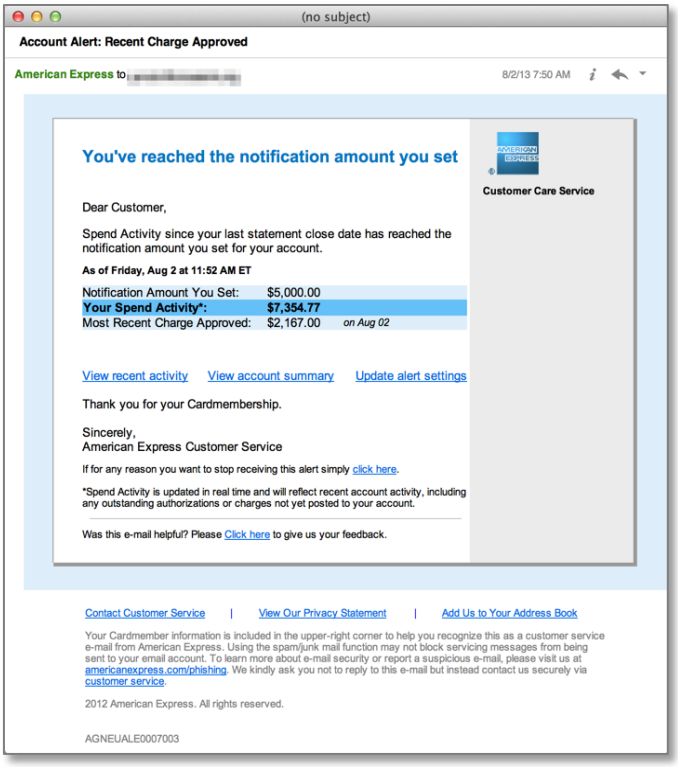
Threat Models

Malvertising

The Online Trust Alliance (OTA) defines Malvertising as "…the cybercriminal practice of injecting malicious or malware laden advertisements into legitimate online advertising networks". Malvertising is a particularly stealthy attack. Bona fide and trusted sites serve up what are thought to be standard ads. In reality, the ads carry malware and the end user is oblivious. By simply visiting a site, users can get infected from a drive-by-download or automatically redirected to a malicious site. Malvertising is particularly hard to detect as most ads are regularly rotated through a site or a specific page and users pay fleeting attention to them, resulting in little or no forensic evidence. Malvertising is also very pervasive; in 2012 the OTA estimates nearly 10 Billion ad impressions were compromised.

Recently, Proofpoint researchers uncovered a malvertising attack being served by the New York Times. It is not unexpected that, given the volume cited earlier, a reputable site such as the New York Times would be affected. Yet the ad's source is surprising; it was served through Google's ad network. Consider the exposure and ad impressions the attackers gain through this use.

Credit Card Longlining Attacks


(no subject)

Account Alert: Recent Charge Approved

American Express to [redacted] 8/2/13 7:50 AM

You've reached the notification amount you set

Customer Care Service

Dear Customer,

Spend Activity since your last statement close date has reached the notification amount you set for your account.

As of Friday, Aug 2 at 11:52 AM ET

Notification Amount You Set:	$5,000.00	
Your Spend Activity*:	$7,354.77	
Most Recent Charge Approved:	$2,167.00	on Aug 02

View recent activity | View account summary | Update alert settings

Thank you for your Cardmembership.

Sincerely,
American Express Customer Service

If for any reason you want to stop receiving this alert simply click here.

*Spend Activity is updated in real time and will reflect recent account activity, including any outstanding authorizations or charges not yet posted to your account.

Was this e-mail helpful? Please Click here to give us your feedback.

Contact Customer Service | View Our Privacy Statement | Add Us to Your Address Book

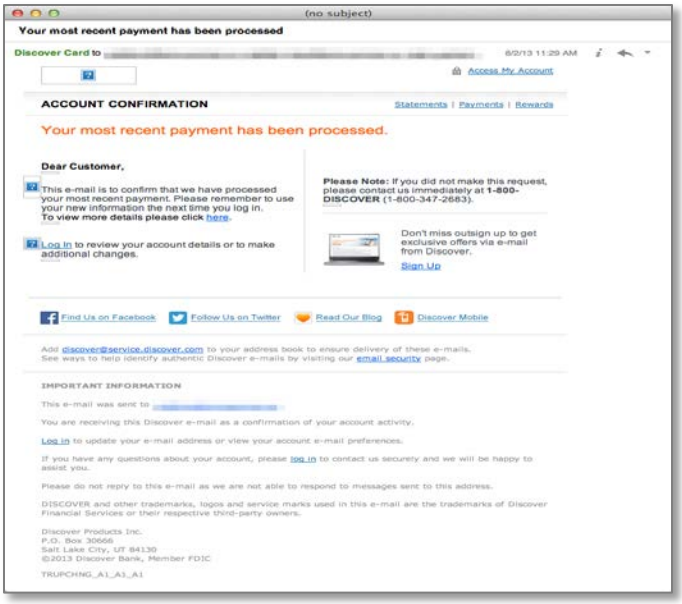
Your Cardmember information is included in the upper-right corner to help you recognize this as a customer service e-mail from American Express. Using the spam/junk mail function may not block servicing messages from being sent to your email account. To learn more about e-mail security or report a suspicious e-mail, please visit us at americanexpress.com/phishing. We kindly ask you not to reply to this e-mail but instead contact us securely via customer service.

2012 American Express. All rights reserved.

AGNEUALE0007003

Recently, attackers used both American Express and Discover Card brands in longlining attacks. Longlining was defined in the January Threat Report and also detailed in the Proofpoint white paper titled - Longline Phishing. Longline phishing attacks are defined by three specific characteristics: 1) Proportionally low volume per organization, with high volume overall 2) Aggressive obfuscation and customization techniques and 3) Malware payloads which utilize unpatched exploits. This was a highly effective campaign, recording a click rate of 24%. The details of the campaign are also interesting.

The email lures were realistic and quite sophisticated with no noticeable errors. The American Express example message contains multiple URLs, and due to its nature and content a high number of users were duped into clicking.


(no subject)

Your most recent payment has been processed

Discover Card to [redacted] 8/2/13 11:29 AM

Access My Account

ACCOUNT CONFIRMATION Statements | Payments | Rewards

Your most recent payment has been processed.

Dear Customer,

This e-mail is to confirm that we have processed your most recent payment. Please remember to use your new information the next time you log in. To view more details please click here.

Log In to review your account details or to make additional changes.

Please Note: If you did not make this request, please contact us immediately at 1-800-DISCOVER (1-800-347-2683).

Don't miss outsign up to get exclusive offers via e-mail from Discover.

Sign Up

Find Us on Facebook | Follow Us on Twitter | Read Our Blog | Discover Mobile

Add discover@service.discover.com to your address book to ensure delivery of these e-mails. See ways to help identify authentic Discover e-mails by visiting our email security page.

IMPORTANT INFORMATION

This e-mail was sent to [redacted]

You are receiving this Discover e-mail as a confirmation of your account activity.

Log In to update your e-mail address or view your account e-mail preferences.

If you have any questions about your account, please log in to contact us securely and we will be happy to assist you.

Please do not reply to this e-mail as we are not able to respond to messages sent to this address.

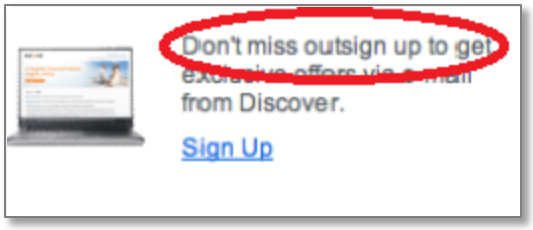
DISCOVER and other trademarks, logos and service marks used in this e-mail are the trademarks of Discover Financial Services or their respective third-party owners.

Discover Products Inc.
P.O. Box 30666
Salt Lake City, UT 84130
©2013 Discover Bank, Member FDIC

TRUPCHNG_A1_A1_A1

A similar Discover card lure was also used in this campaign. At first read it's as sophisticated as the AMEX lure.

However, on very close examination, spelling and grammar mistakes are found:



The campaign consisted of 159,147 messages. They were sent using 3,040 different sender

addresses from 8,555 IPs. There were 87 compromised websites and 916 unique URLs utilized.

The URL pattern is one Proofpoint researchers identified in other attacks:

```
http://<compromised website>/<random dictionary word>/index.html
```

For example, a single compromised server might have the following URLs used in one campaign:

http://www.urmel-kinderladen.de/baronial/index.html
http://www.urmel-kinderladen.de/centrifuging/index.html
http://www.urmel-kinderladen.de/chug/index.html
http://www.urmel-kinderladen.de/disenchants/index.html
http://www.urmel-kinderladen.de/foldaway/index.html

Notice every URL ends in index.html, a common page name.

As stated earlier, this campaign garnered an impressive 24% click rate; a high rate and therefore successful campaign. The lures were delivered on Friday, August 2nd, but notably, a majority of the clicks were recorded on Saturday, August 3rd and tailed off into Monday. Most, if not all, weekend clicks occurred at a home office, or coffee shop, somewhere off the corporate network. It's vital to consider usage patterns and to protect users both on and off the corporate network. Proofpoint Targeted Attack Protection delivers this level of protection.

Threat News

Backdoors via Image Files

Attackers are using a known, but unusual exploit to maintain control over compromised web sites, researchers at Sucuri have found. They are utilizing backdoors hiding in the headers of image files. Sites running either WordPress, a popular blogging platform, or Joomla, a competitor, are both mentioned as affected. The headers of the image files were modified to enable remote execution of "a function that will execute any content delivered to it via POST. Using this, an attacker can issue commands, or call for shell scripts hosted remotely and execute them." The full article is available on CSO Online at http://www.csoonline.com/article/736622/attackers-embedding-backdoors-into-image-files

Another Type of Attack: Watering Holes

Watering hole attacks are perpetrated via industry, profession (i.e. journalism), or other personal interest web sites. Similar to a watering hole in nature, the hunter knows the prey must come to drink at some point, and so they lie in wait. As the user visits the compromised site, they are unknowingly redirected to the malicious hosts. In the case cited in this article;

http://www.infosecurity-magazine.com/view/28450/the-voho-campaign-gh0st-rat-spread-by-waterholing RSA researchers exposed a waterhole attack that infected 12% of the visiting population to such a site.

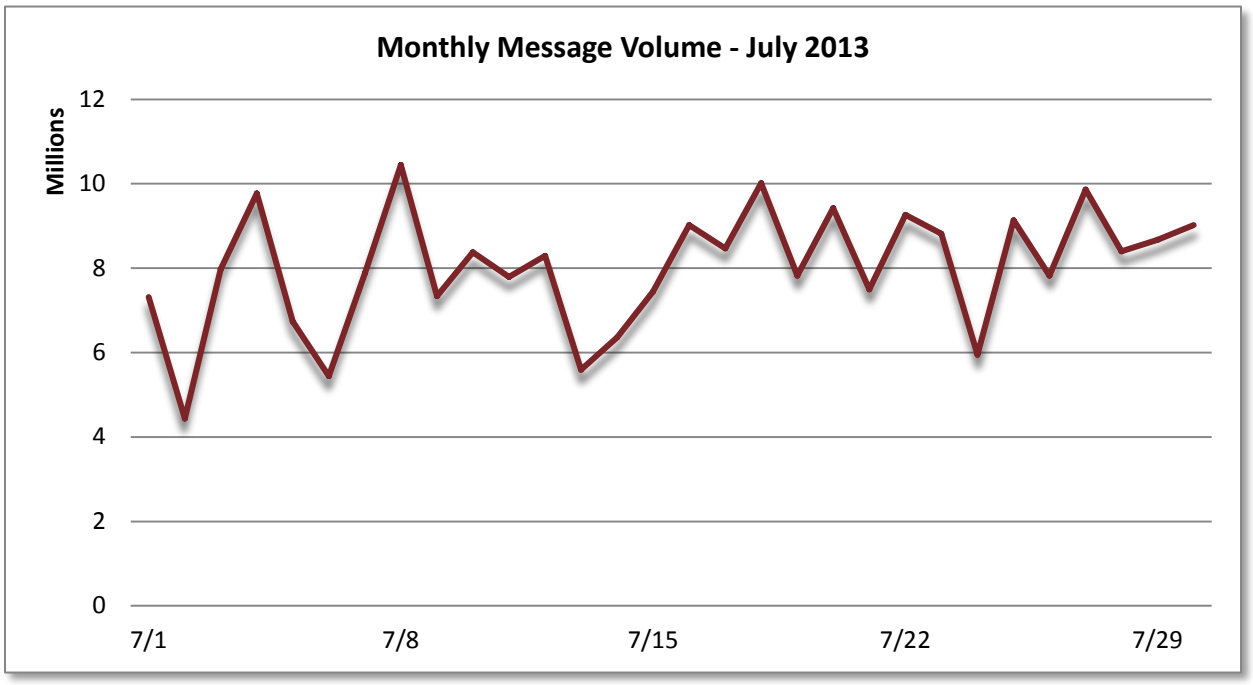
Interactive Infographic – World's Biggest Data Breaches

Data breaches are another form of security breach. There are daily news reports of organizations both private and public exposing end user, customer or patient data. It is hard to grasp the volume of the data breach problem. The team at "Information is Beautiful" has published one of the most informative and interactive infographic covering data breaches, providing multiple filters. Details of each breach can be located with a simple click on each bubble.
http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

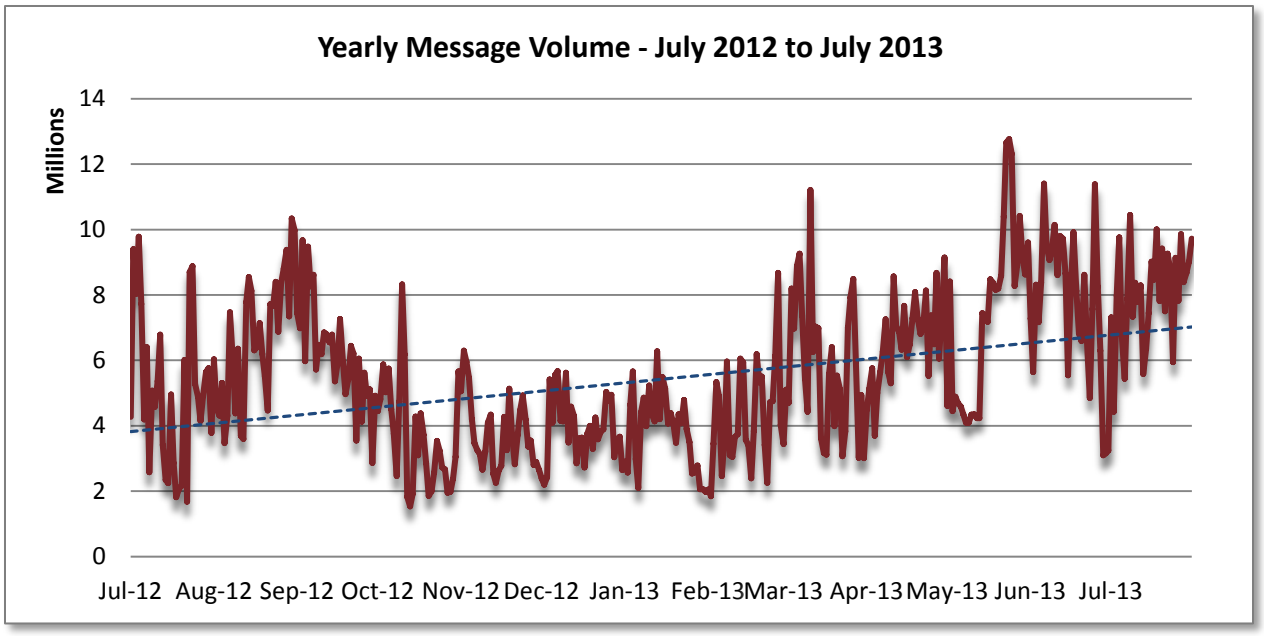
Threat Trends

Spam Volume Trends

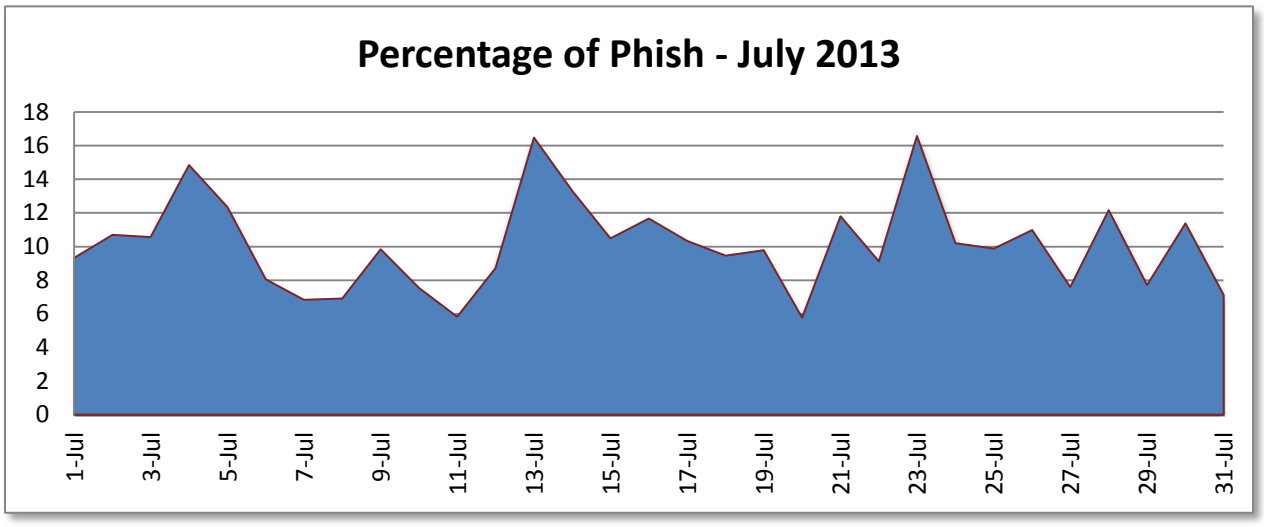
Proofpoint tracks spam volumes via a system of honeypots. These spam volumes have historically tracked closely with that of our customer base. Spam increased again in July. Unlike June where spam volumes presented an erratic pattern all month, July volumes remained in a narrower range. Four volume spikes near or above 10 million messages per day occurred during the month on Proofpoint honeypots. Each occurrence can be seen in the graph below.



July set a new yearly high for the third month running. June to July volumes increased by 3.74% - the sixth monthly increase in a row. July recorded a 60.51% year over year increase from July of last year, the largest year over year increase in over two years. Spam volumes have increased a full 109% from the beginning of 2013. The trend continues a strong upward trajectory.



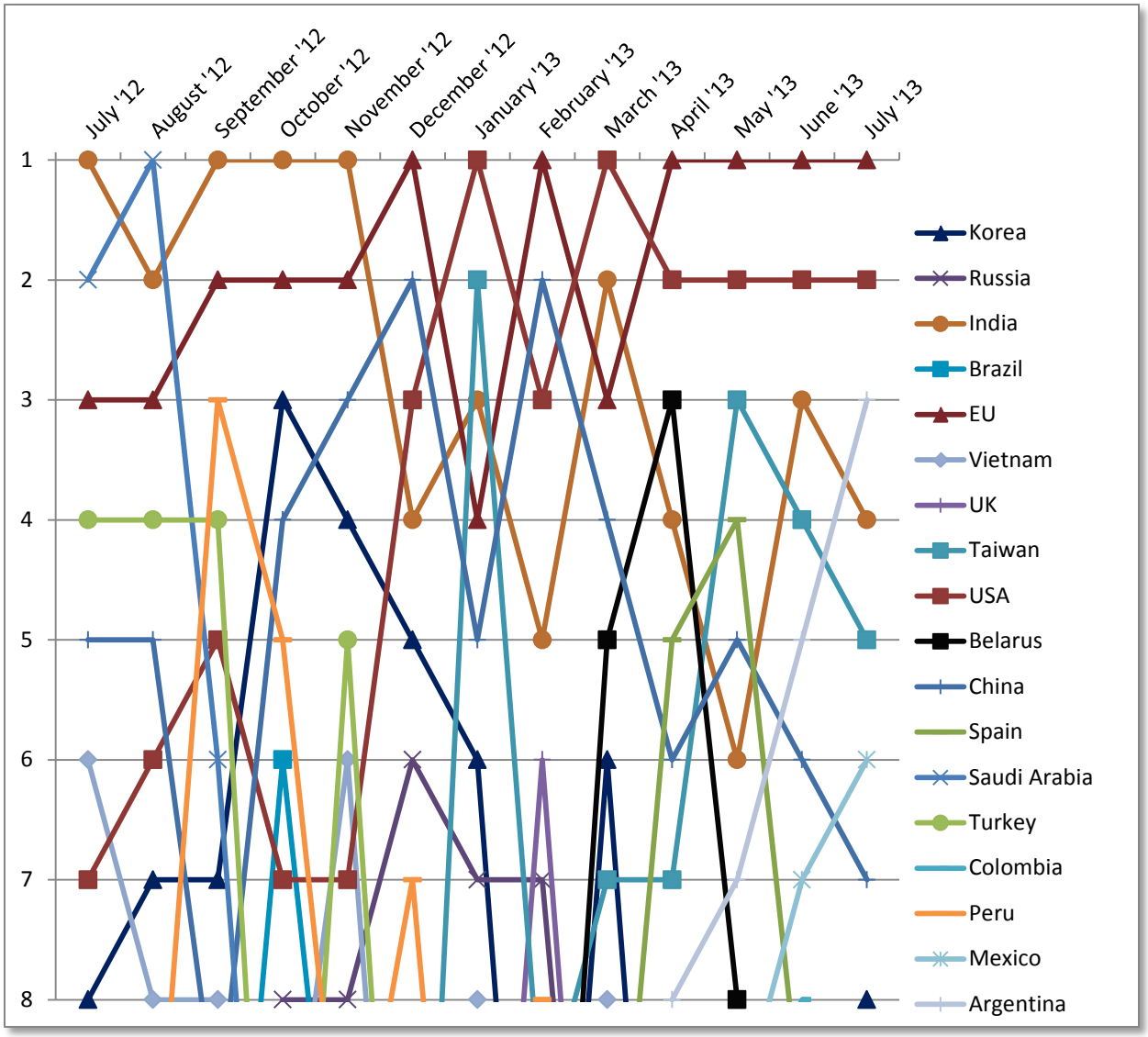
Phish Classification Trends



The average percent of daily messages classified as phish by Proofpoint's MLX technology continued a downward trend in July. July saw three daily spikes, the same as in June, and the highest spike reached 16.57% on the 23rd. In contrast, two of the three June spikes topped 18% of daily message volume. On average in July, 10.11% of daily message volumes were classified as phish; a 2.5% decrease in standard phish messages from June.

Spam Sources by Country

The European Union again ranks as the number one spam source in July 2013. The United States remains the #2 source of spam. This marks four straight months where the first and second spots remained unchanged. Argentina moved up two slots to number three. The following chart shows the historic trend of the top spam sending countries.



In the table below are the leading spam senders for the months of June and July, ranked by % of the total spam volume.

June 2013			July 2013		
1	EU	15.88%	1	EU	17.76%
2	USA	5.71%	**2**	USA	7.05%
3	India	5.38%	**3**	Argentina	5.19%
4	Taiwan	5.01%	**4**	India	4.31%
5	Argentina	4.58%	**5**	Taiwan	3.80%
6	China	3.53%	**6**	Mexico	3.37%
7	Mexico	3.29%	**7**	China	3.14%
8	Columbia	2.75%	**8**	Korea	3.02%

proofpoint

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