proofpoint

Proofpoint Threat Report

July 2014

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

Threat Models

Grand-Scale Pharma Spam Campaign Sent from a Large Botnet

Over the last few weeks, the Proofpoint spam team has been monitoring an evolving pharma (pharmaceutical) spam campaign similar to last month's stock pitch spam campaigns. While the pharma campaign is of a lesser magnitude, it still poses a threat to users. As always, Proofpoint is actively dealing with the new iterations as they appear, adding updates to our spam definitions as well as creating new predictive rules.

Sample campaigns are highlighted below.

Campaign #1

A large botnet attack hit Proofpoint spamtraps on Thursday, July 10, 2014 at around 7:33 a.m. PDT. The messages consistently claimed to be from addresses beginning with the letter "v", but was actually sent from varied, random addresses, like those shown below:

1. From: venita.a@email-discounts[.]com <numerator@flora.waw[.]pl>
2. From: vera.schuster@championoffers[.]com <vlsnf@bizjunction[.]com>
3. From: veralinss@net-submissions[.]com <marek.wrzoskowicz@howden[.]pl>
4. From: ve@ticmail[.]net <euroauton@toquero[.]com>
5. From: veils539@nyetmail[.]com <m.gajda@grand-hotel[.]pl>
6. From: vrx4xclo@wittyhenrys[.]us <seagonzo@globalcrossing[.]net>

The *Subject* contained multiple variants of the same pharma phrase. Examples follow:

1. Subject: Int///ernaational me///dst0re o///ni|ne
2. Subject: Int///ern@tional me///sdtore o///nliine
3. Subject: Int///ernatioonal me///d$tore 0///nl1ne
4. Subject: Int///ernaitonal me///dst0re 0///nl|ne
5. Subject: Int///ernaational md///estore o///nlnie
6. Subject: Int///ernaational me///dst0re 0///n1ine

Slashes have been added to prevent the phrase (and this report) from being caught as spam.

The URL payloads were as follows:

- hxxp://doctorswmb.cn[.]com/?[randomstring]
- hxxp://doctorswmb.cn[.]com/?[randomstring]

This campaign was blocked with spam definitions minutes after it began.

Sample Message

```
Internaitonal medstroe onilne
hxxp://doctorswmb.cn[.]com/?jhjgffdsh
```

Campaign #2

The second variation surfaced on the same day at 7:50 a.m. PDT. It was also a large botnet attack. The messages consistently claimed to be from "VIP PfizerClub", but in actuality, were from seemingly random addresses:

1. From: "VIP PfizerClub" <gamed1376@bell[.]ca>
2. From: "VIP PfizerClub" <ynchuck846@business.telecomitalia[.]it>
3. From: "VIP PfizerClub" <stleigh.sheeksc6c@advico[.]co.uk>
4. From: "VIP PfizerClub" <chuck1f07@co[.]za>
5. From: "VIP PfizerClub" <fadamsnn37@82-198-197-167.briteline[.]de>
6. From: "VIP PfizerClub" <bernadetted76@dialog{.}net.pl>

Following is a list of example *Subjects*:

1. 5 h///ot days of ab///solutely fan///tastic SALE
2. Per///fect sa///ving s///olution! Onl///ine sh///opping!
3. Sav///ing and sh///opping is the b///est this week!
4. Wis///e fu///nds d///istribution inc///ludes SA///LE s///hopping!
5. We sel///l all pr///oducts o///nline at lea///st tw///ice c///heaper!
6. The bes///t on///line o///ffer of the mon///th! 75///% d///iscounts!

The URL payload patterns were as follows:

- hxxp://[random username from *To:* address].homeherbsservice[.]ru/?[randomstring]
- hxxp://[random username from *To:* address].hotcurativemart[.]ru/?[randomstring]

Another successful block via spam definitions took place shortly after this campaign began.

Sample Message

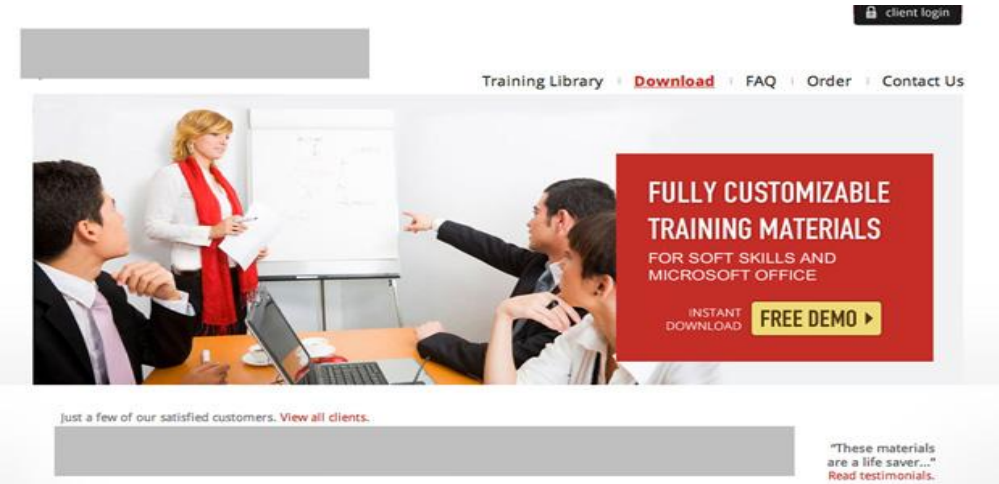
```
      The more you order the cheaper you get it. The
faster you visit us the better is the choice!

      hxxp://[random username from To:
address].homeherbsservice[.]ru/?[randomstring]
```

Teach a Man to Phish

Employee training and development is critical to the well-being of organizations of all sizes and in all industries. Consequently, keen management is on the lookout for new and effective educational tools for its employees.

Proofpoint researchers recently detected malware hidden in the website of a provider of corporate training tools via links in URLs sent to director-level employees of a large health care organization.



This “watering hole” attack enables phishers to leverage legitimate e-mail while avoiding the grammatical errors and amateurish visuals that employees have been trained to recognize as signs of phishing. Additionally, watering holes can enhance phishing effectiveness because the e-mails do not include any financial account alerts, registration links, social network connection requests, or other hallmarks of the most common phishing templates. All of these factors combine to alleviate suspicion and increase the likelihood of a user’s click-through to the malicious site.

An analysis of this site, which was flagged as a result of user clicks on e-mailed links, reveals that clicking on the link causes redirection to a Russian traffic direction system (TDS) that for the last month has been redirecting clients to an instance of the Sweet Orange exploit kit. In addition to leveraging a wide range of the most current exploits, this exploit-kit-for-hire also employs encryption to obfuscate its malware in order to improve the chance of evading detection by anti-virus engines at the client and gateway. This particular instance delivers the QBOT malware, which steals banking credentials and encryption certificates, while it spreads to other systems on the local network via open file shares—and acts as a keylogger, backdoor, and downloader for future malware.

While employee education is an important part of the defense against modern, sophisticated phishing attacks, this detection offers a lesson in the challenges of keeping up with today’s threats. Targeted phishing campaigns that use watering holes highlight the ways in which attackers are continually learning (and evolving) to leverage not only the latest exploits and technology, but an understanding of the business needs of managers and organizations in order to improve the effectiveness of their phishing campaigns.

Threat News

The Psychology of Phishing

In the following article, Proofpoint’s very own Mark Sparshott, EMEA (Europe, Middle East, and Africa) Director, examines the psychology and the methodology of phishing.

By a wide margin, one of the biggest threats to consumers and organizations is phishing e-mail. Gone are the “good ol’ days” when cybercriminals would send out thousands of e-mails at random, in hopes of getting a sprinkling of hits. Today’s phishing e-mail is highly targeted, and created with the recipient in mind, albeit a far more tedious process. Finely crafted e-mail undoubtedly provides a greater return on the criminals’ investment.

Understand cybercriminal psychology, read the results of Proofpoint's "Human Factor" research, and pay close attention to Mark's instructions by clicking here: http://www.net-security.org/article.php?id=2078.

Cyber Fraudsters Tweet Malicious MH17 URLs Hours After Incident

Predictably, cybercriminals have jumped onto the tragedy bandwagon once again by embracing the downing of Malaysia Airlines Flight 17 to trick users into clicking on spammy, malicious Twitter links. Clearly, these could lead to malware infection.

Exploiting major breaking news and gossip such as this one, for illegal gain, is nothing new. Cybercriminals have always been among the first to react. They feed off of human curiosity for profit.

The details can be found here: http://www.infosecurity-magazine.com/view/39391/cyber-fraudsters-tweet-malicious-mh17-urls-hours-after-incident/.

Threat Insight Blog

Here we highlight interesting posts from Proofpoint's threat blog, *Threat Insight*. Subscribe to *Threat Insight* and join the conversation at http://www.proofpoint.com/threatinsight.

Fiesta Where?

On occasion, there is humor to be found in the world of commercial crimeware.

A recent example of this occurred when Proofpoint detected an e-mail with a link to a website featuring a recipe for a Tex Mex Frito salad. Sandboxing revealed that it linked to an infected webpage. This webpage, in turn, redirected to a link serving the Fiesta (NeoSploit) exploit kit.

While the example above was most likely a coincidence, it begs the question: could such coincidences inspire a phisher with a sense of humor? In this case, perhaps a Fiesta dinnerware site may be slated to be infected.

For additional information on the Fiesta exploit kit and exploit kits in general, please read on: http://www.proofpoint.com/threatinsight/posts/the-fiesta-exploit-kit.php.

Phishers Keep It Simple

Not so long ago, we wrote about a credential phish that employed a valid SSL certificate and an almost perfect replica of a Google login page to trick users into entering their Google credentials.

Proofpoint researchers detected yet another campaign that expands on this approach, with some devious twists. As in the previous case, the user receives a generic e-mail that directs him to his e-mail account login. Here, the URL is dynamically generated and unique to each message, with base64-encoded strings that represent the recipient's e-mail address and username.

Note that the domain hosting these pages was created *on the morning of the very same day* that Proofpoint detected the campaign.

For the details, click here: http://www.proofpoint.com/threatinsight/posts/phishers-keep-it-simple.php.

Destination Malware: Travelers Targeted by Infected Travel Websites

Proofpoint security researchers were recently the first to discover that a large number of travel-related websites had been compromised and used to deliver the Nuclear exploit kit.

Proofpoint Targeted Attack Protection (TAP) detected the infected sites after users received a promotional e-mail containing links to infected pages. This has most likely been an effective campaign, and it shares many of the attributes usually associated with watering-hole attacks, since these were legitimate e-mails that users had opted to receive.

Shrewdly and fittingly, some of the promotional e-mails included references to Independence Day activities, while others were simply general travel-related content. The attackers timed their shenanigans to coincide with the season.

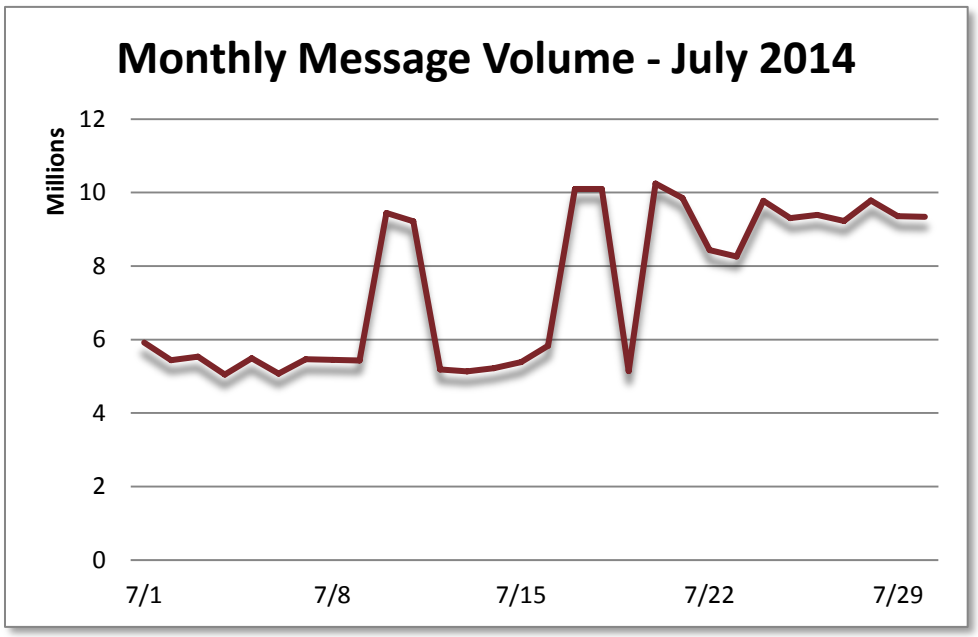
Get the scoop here: http://www.proofpoint.com/threatinsight/posts/travelers-targeted-by-infected-travel-websites.php.

Threat Trends

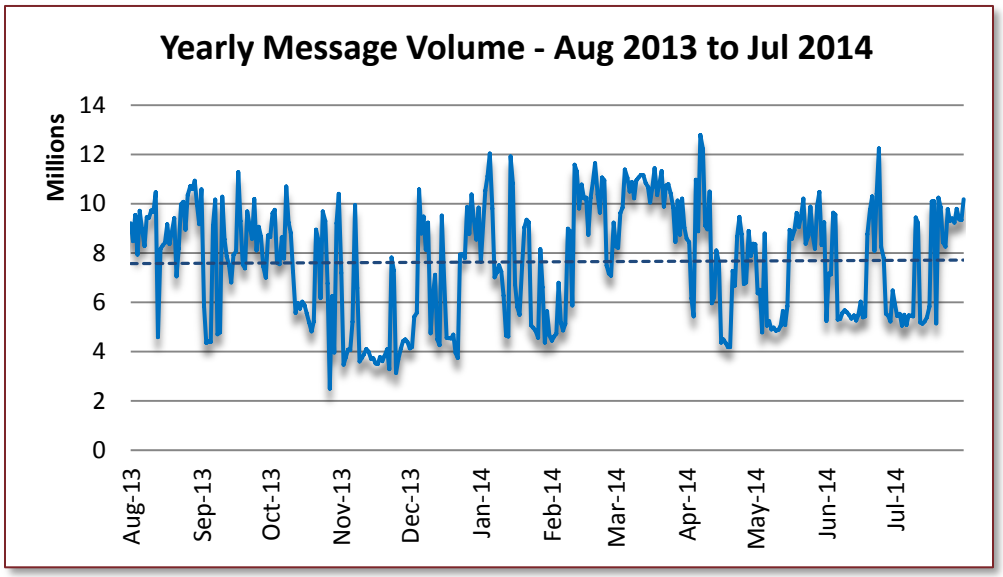
Spam Volume Trends

Proofpoint tracks spam volumes via a system of honeypots. The volumes historically track with that of our customer base. July's daily spam volumes remained somewhat static during the first week but began to fluctuate dramatically at the start of the second. Volumes were below 6 million/day and immediately rose to a whopping 9 million/day. The middle of the second week

witnessed more drama as the spike catapulted to its former position, of less than 6 million/day. But the most dramatic upswing occurred at the beginning of the third week, as it exceeded previous high at approximately 10 million/day, followed by another downswing to roughly 5 million/day in the middle of the third week. One last spike gained tremendous momentum to return to 10 million/day near the end of the third week. Slight vacillations capped the fourth week as the month closed at a level 9 million/day.



By comparison, June over July demonstrated an increase in volume. The volume of spam increased by 8.12%. The year over year tally was at -6.87%.



Spam Sources by Country

While the EU rose to the occasion in July, the US recaptured the coveted second position in the Top Five. Unsurprisingly, the third slot went to China, while Argentina stepped up its game to capture fourth, and the fifth went to Russia.

The following table shows the Top Five spam-sending continents and countries for the last six months.

		Feb '14	Mar '14	Apr '14	May '14	Jun '14	Jul '14
Rank	1st	EU	EU	EU	EU	EU	EU
	2nd	US	US	Argentina	US	Vietnam	US
	3rd	Argentina	Argentina	US	Argentina	US	China
	4th	Russia	India	Russia	Russia	China	Argentina
	5th	China	Mexico	China	China	Russia	Russia

The table below details the percentage of total spam volume for the June and July 2014 rankings noted above. The calculation of the volume for the EU is based on the inclusion of all member states, thereby producing a better representation of its volume. At 38.13%, the European Union continues to generate the grand majority of the world's spam. The remaining four countries in the top five slots were collectively responsible for 20.32%—slightly more than half the output of the EU.

June 2014			July 2014		
1	EU	30.89%	**1**	EU	38.13%
2	Vietnam	5.91%	**2**	US	6.94%
3	US	5.53%	**3**	China	5.19%
4	China	5.25%	**4**	Argentina	4.58%
5	Russia	4.70%	**5**	Russia	3.61%

threat insight

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

