proofpoint

Proofpoint Threat Report

August 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

How Can You Stop a Broken Spam Campaign?

Recently, the Proofpoint spam team monitored a large-scale, broken spam campaign. In short order, Proofpoint engineers released several updates to our spam definitions to combat the campaign.

This campaign is of particular interest and significance because there was no payload (URL or attachment), or other call to action. Despite that fact, Proofpoint detected this challenging campaign with relative ease. It was sent from a very large botnet that involved around 40,000 unique and unused IP addresses and hit our spamtraps on Tuesday, August 26, 2014 at around 2:50 AM PDT.

The messages contained a random *Subject* line and two to three lines of random body text. All of the *Subjects* had an exact match on Google to a wiki or encyclopedia entry, and ended with a literal period.

Sample Message

```
     Dear little snowflake, soft and white. The 2000
Census reported a total population of 2,128 for all of
Mapleton Township. Barbana Hospital was opened. Her
next tournament was Moscow, where she was seeded
second.
```

Curiosity Clicks: Using Bitcoin's Hype for Phishing Fun

The world of the crypto-currency Bitcoin stands in stark contrast to that of heavily regulated and policed government-backed currencies and online banking and payment services. Unregulated and designed for anonymity, Bitcoin represents a handsome $6.8 billion target—and a bonanza to cyber criminals.

Blockchain.info, the most popular Bitcoin website, reports that since September 2013, the number of users has grown exponentially to over 2,000,000 users and daily transactions have nearly tripled to over 30,000 per day.

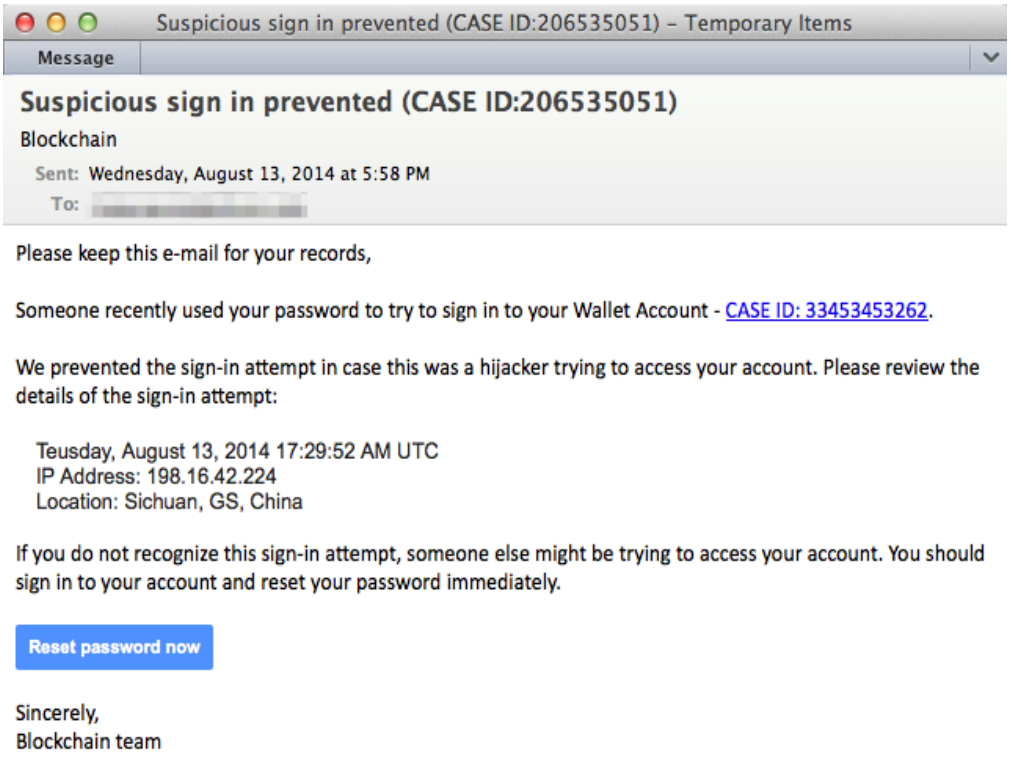
In light of its increased popularity, phishing attacks targeting Bitcoin users have become more frequent. Perpetrators are using lists of known and active Bitcoin users or leveraging popular misperceptions involving Bitcoin to try to improve their odds of success. Note that attacks generally take the form of credential phishes.

While many people have heard of Bitcoin, it is not yet in mainstream use. Consequently, Proofpoint researchers were recently surprised to detect a Bitcoin credential phishing campaign. It received a 2.7% click-through rate. This is much higher than the percentage of Bitcoin users in the general public.

Proofpoint went on to detect 12,000 messages in this campaign. Sent in two separate waves to over 400 organizations in a range of industries, including education, financial services, technology, media, and manufacturing, the breadth of this campaign was surprising since most of the other Bitcoin phishing attacks have targeted known users of Bitcoin.

The phishing e-mail follows a fairly straightforward "account warning" template. It uses the Bitcoin site (blockchain.info) instead of one of the usual bank or online payment service names. The message itself acts as a warning to the recipient that there was a failed login attempt originating in China. It attempts to inject a sense of urgency by capitalizing on popular fears over Chinese hacking. A legitimate-looking "case ID" is also presented.

Sample Message


Suspicious sign in prevented (CASE ID:206535051) – Temporary Items

Message

Suspicious sign in prevented (CASE ID:206535051)

Blockchain

Sent: Wednesday, August 13, 2014 at 5:58 PM

To:

Please keep this e-mail for your records,

Someone recently used your password to try to sign in to your Wallet Account - CASE ID: 33453453262.

We prevented the sign-in attempt in case this was a hijacker trying to access your account. Please review the details of the sign-in attempt:

Teusday, August 13, 2014 17:29:52 AM UTC
IP Address: 198.16.42.224
Location: Sichuan, GS, China

If you do not recognize this sign-in attempt, someone else might be trying to access your account. You should sign in to your account and reset your password immediately.

Reset password now

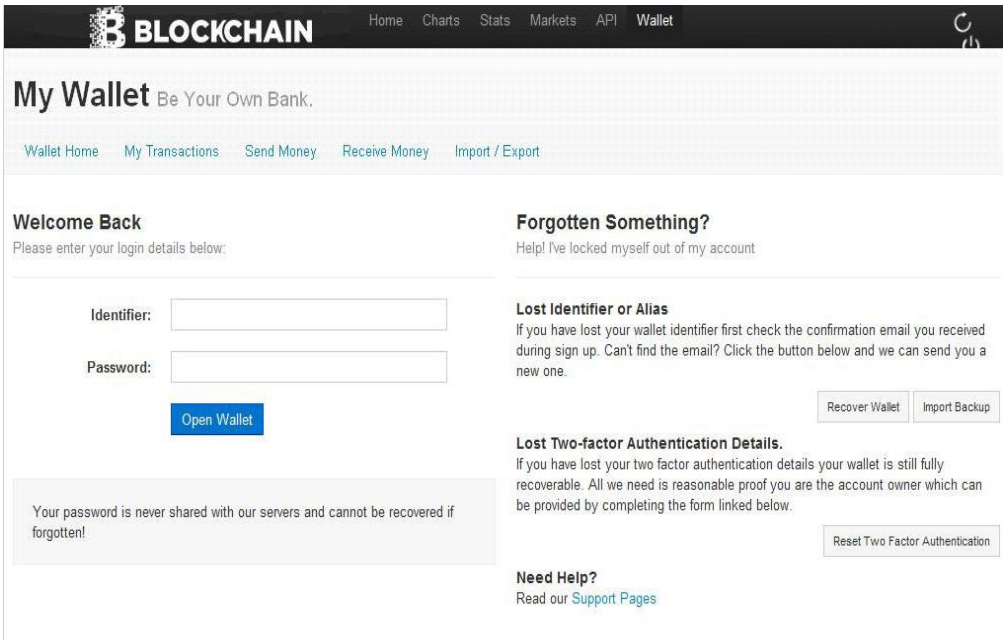
Sincerely,
Blockchain team

Over two days, the campaign tactics iterated in a fashion typical of modern phishing campaigns. While the message and the content remained unchanged, the use of URLs shifted:

- On the first day, the campaign used a single hostname (blockchain.info) within URLs that were individually randomized with a custom parameter for each e-mail.
- On day two, the randomized URLs featured multiple, unique *.com* domains (e.g., http://blockchain [dot] info [dot] caseid832482834 [dot] com). These had been generated and registered in advance. (The cycling of multiple, newly created domains improves the attackers' odds of evading reputation-based blocking.)

This shift in domains is likely due to the initial countermeasures Proofpoint took after the attack began.

The fact that 2.7% of the recipients clicked on the link makes it likely that a mix of both Bitcoin and non-Bitcoin users were clicking on this phishing e-mail. Clicking the *Reset Password* button in the messages sends the recipient to a realistic but fake Blockchain login page:



Any information entered into this page by the user would be captured and sent immediately to the phishing attackers, while the user is sent to a generic login error message. Once equipped with this information, the attackers can log in to the user's real account and send bitcoin to any wallet that they want. Because Bitcoin transactions are, by design, irreversible and difficult to trace, the victim has almost no recourse. Moreover, the regulations that protect consumers from loss attributable to online banking fraud does not apply to Bitcoin, making it unlikely that a Bitcoin thief will have to contend with pursuit by the banks.

This simple but effective phishing campaign demonstrates that security professionals can't afford to discount any phishing e-mails, even consumer-based messages that don't appear to be relevant to their end users, because *effective lures attract clicks even from users who should have no reason to click*.

Threat News

Hundreds of Norwegian Energy Companies Hit by Cyber-attacks

Approximately three hundred oil and energy companies in Norway have been hit by one of the biggest cyber-attacks of all time in the country, according to a government official.

Norwegian shores were last targeted heavily in 2011. Ten oil, gas, and defense-sector enterprises were struck via spearphishing e-mails. The unidentified hackers made off with industrial drawings, contracts, and login credentials.

In response to the recent news, Alan Calder, founder and executive chairman of IT Governance, stated the following to *SC Magazine UK*:

"Spearphishing attacks—increasingly through the compromised systems of small suppliers to large companies—is an increasingly interesting attack vector for criminals attempting to steal valuable information and IP."

Continue reading this enlightening article.
http://www.scmagazineuk.com/hundreds-of-norwegian-energy-companies-hit-by-cyber-attacks/article/368539/

Cryptolocker Victims to Get Files Back for Free

Thanks to security firms FireEye and Fox-IT, an online portal has been created to facilitate recovery efforts for victims of the Cryptolocker threat, free of charge.

DecryptCryptolocker.com was created after security researchers managed to obtain a copy of Cryptolocker's database of victims.

Recently, law enforcement agencies and security companies seized a worldwide network of hijacked home computers that was being used to spread both Cryptolocker and another strain of malware called Gameover ZeuS.

Cryptolocker was first spotted in September 2013.

It is a prolific and very damaging strain of malware. It uses strong encryption to lock files that are likely to be the most valued by victims: Microsoft Office documents, photos, and MP3 files.

A warning is typically presented on infected machines, indicating locked files. These can only be decrypted by sending a certain fraction/number of *Bitcoins* (digital currency) to a decryption service run by the perpetrators. Victims are given 72 hours to pay the ransom—typically a few hundred dollars in Bitcoins—after which the ransom ratchets upward fivefold or more.

To learn more, click ahead: http://www.bbc.com/news/technology-28661463

How Do Hackers Breach Institutions Like Canada's NRC?

Being on the digital defensive has increasingly become a cat-and-mouse game.

Cyberattacks, such as the one against the National Research Council of Canada (NRC), are increasing. To have the upper hand in the fight, security experts strive to determine the attack's strategy.

In the following article, an ethical hacker explains the complicated apparatus that is a cyberattack. He breaks down the process into six steps, each of which is used in the more sophisticated jobs.

This presentation offers a glimpse of the methodology by which the hacker operates. http://www.ctvnews.ca/sci-tech/how-do-hackers-breach-institutions-like-canada-s-nrc-1.1938113

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.

What's Your Vector of Choice? PDF, Word, or ZIP?

Perpetrators continually use advanced tactics to extract maximum performance and value from their campaigns.

In recent months, Proofpoint engineers have been tracking a particular threat actor. The weapon of choice has been PDF files that exploit the CVE-2013-2729 vulnerability. The campaign began with large e-mail runs containing malicious PDF files; however, over the months, the maneuvers have become more diversified. Instead of using a single attack vector, the perpetrator has delivered the same malware via multiple approaches. Proofpoint engineers observed e-mails with the following combinations:

- URL to malicious PDF file plus URL to malware inside a ZIP file
- Attached PDF file plus URL to malware inside a ZIP file
- Attached PDF file plus URL to malicious Word document (CVE-2012-0158)
- Attached ZIP file with malware

Further detail, closing remarks, and some example e-mails follow.
http://www.proofpoint.com/threatinsight/posts/whats-your-vector-of-choice.php

Cashing in on Ebola: How Scammers Use Fear to Infect Users

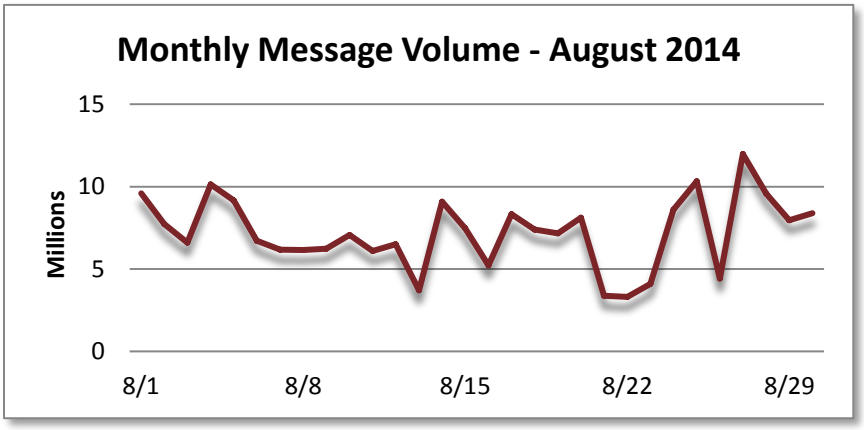
Proofpoint security researchers discovered an e-mail campaign that attempted to capitalize on the recent outbreak of Ebola to infect users with a banking trojan. Since infectious disease epidemics can cause the kind of fear that leads to frantic Web searches and emotion-driven clicking, such attacks can be particularly effective. In this campaign, the attackers created an exact copy of the World Health Organization (WHO) Ebola "factsheet" site and sent phishing e-mails to unsuspecting users. If the users clicked links in the lure e-mail, the site would download a Java payload and execute malware that appears to be a Zeus variant.

Take a look at the e-mail template here.
http://www.proofpoint.com/threatinsight/posts/ebola-threat-banking-trojan.php

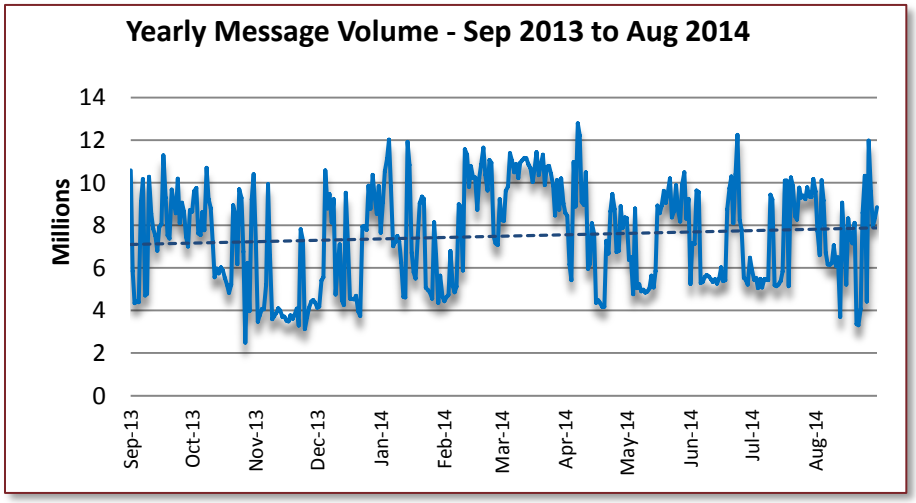
Threat Trends

Spam Volume Trends

Proofpoint tracks spam volumes via a system of honeypots. The volumes historically track with that of our customer base. August's daily spam volumes plummeted at the beginning of the first week and then catapulted to over 10 million by midweek. A fairly constant decline ensued until the level plateaued at 6 million/day. Vacillations occurred through the middle of the second week, then dipped below 4 million. The third week saw a spike to 9 million/day, holding roughly steady through the week, coming in at under 4 million/day by the end of the week. The greatest of upswing occurred at the beginning of the fourth week, with a high of over 10 million/day, which then plummeted to just above 4 million/day. One last massive spike to 12 million/day ended the final week. A slight downward trend capped the month at just above 8 million/day.



By comparison, July-over-August demonstrated a 3.19% decrease in the volume of spam. The year-over-year tally was a whopping negative 20.09%.



Spam Sources by Country

While the EU rose to the occasion in August, the US recaptured the second position in the top five. Argentina regained momentum and stole third, while Russia and China captured fourth and fifth, respectively.

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

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

The table below details the percentage of total spam volume for the July and August 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 39.33%, the European Union continues to generate the lion's share of the world's spam. The remaining four countries in the top five slots were collectively responsible for 17.88%—less than half the output of the EU.

July 2014			August 2014		
1	EU	38.13%	**1**	EU	39.33%
2	US	6.94%	**2**	US	7.31%
3	China	5.19%	**3**	Argentina	4.82%
4	Argentina	4.58%	**4**	Russia	3.17%
5	Russia	3.61%	**5**	China	2.58%

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

