proofpoint

Proofpoint Threat Report

April 2015

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 Human Factor 2015: Attackers Drive Business End-User Clicks

In 2014, Proofpoint published *The Human Factor* research report (https://www.proofpoint.com/us/human-factor-2014). The white paper, by Proofpoint threat experts, documents the results of a wide-ranging study that reveals the role of the end-user in email-borne threats. It is tempered by a new awareness of the harsh realities via a unique, data-driven view.

The study examined exactly who was clicking on the malicious links in emails, identified the most effective click-precipitating email templates, captured where users were clicking, when they were most likely to click, and ultimately, why they clicked on malicious URLs at such a high rate.

Evidence supports that company staffs were clicking on social media "invitation" (phishing) messages delivered in a flood before the start of business. Twenty percent of these clicks took place outside the corporate network.

The new findings can be viewed in *The Human Factor* report for 2015 (https://www.proofpoint.com/us/id/WP-Human-Factor-Report-1).

In particular, the findings unveil that in 2014, widespread end-user education gave rise to new thinking about phishing as a threat, thus empowering end-users to:

1. Recognize the most common phishing templates.
2. Be wary of unsolicited messages in general.

In response to a greater awareness of the existence of fraud, the evildoers shifted their strategy to focus on the exploitation of middle management. By the end of 2014, cyber criminals were targeting subtly different user populations whilst employing new maneuvers. For a blog post detailing a glimpse of the shenanigans, continue reading: https://www.proofpoint.com/us/threat-insight/post/The-Human-Factor-2015.

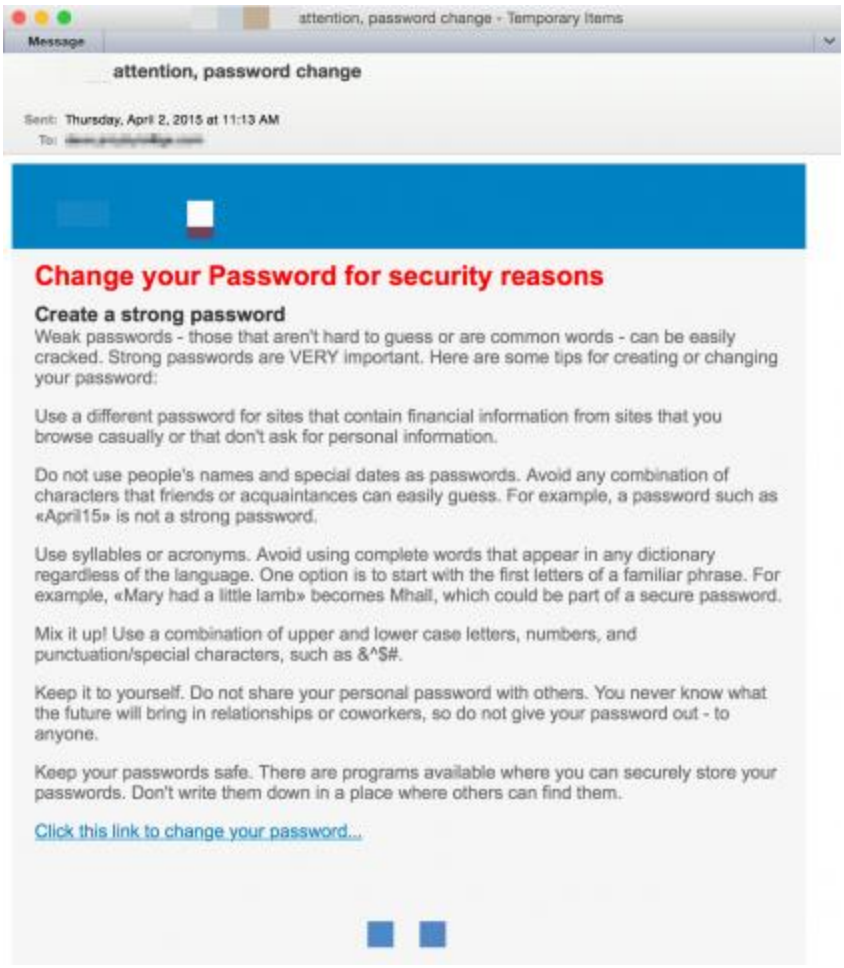
Fraud Feeds Phishing in Tax-Themed Email Campaign

Earlier this year, Proofpoint researchers analyzed some tax-themed phishing lures (https://www.proofpoint.com/us/threat-insight/post/Tax-Return-Malware-Attacks) that revealed that perpetrators were filing their "returns" early in hopes of capitalizing on recipients' fear or curiosity. A mere click of the malicious link or attachment would be the end-all. Intriguingly, one of the lures even manifested a combination of phishing e-mail, malicious link, and telephone-based social engineering and was spotted in a recent, sophisticated Dyre campaign (https://threatpost.com/dyre-banking-malware-a-million-dollar-threat/112009).

With the recent tax season, and with many in a quandary over fraudulent tax return filings (http://www.wsj.com/articles/fraud-alert-what-turbotax-users-need-to-know-now-1423847170), Proofpoint researchers have observed attackers shift lures from IRS-themed communications to tax-filing tool lures with a fraud-prevention theme. For example, the researchers recently detected variant emails purporting to be password reset reminders from a popular tax-filing software package. But instead, they lead to the Angler exploit kit.

The campaign was relatively targeted, considering that the volume of messages was well below the hundreds of thousands normally observed for unsolicited email campaigns.

The lures, well-written and convincing, were designed to play on popular fears of phony tax filings:



Clicking the link redirects to an Angler exploit kit (EK) server.

Notably, all of the URLs observed in this campaign had low detection rates due to the fact that the link in every message led to a unique hostname.

And finally, if the EK can successfully execute an exploit, it installs the Bedep Trojan (http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Win32/Bedep#tab=2).

It mainly functions as a downloader, data stealer, and advertising fraud tool.

Benjamin Franklin once said, “In this world nothing can be said to be certain, except death and taxes.”

But just as certain are cybercriminals who target, adapt, manipulate, and ultimately, control. In this case, heightened awareness of one kind of fraud gave rise to a lure for another. *Touché*.

Threat News

FCC Fines AT&T $25M for Call Center Breaches

The Federal Communications Commission used the iron hand in the velvet glove to assert its information privacy authority by reaching a significant settlement with AT&T over data breaches in 2013 and 2014 at a group of call centers in Colombia, Mexico, and the Philippines. Information on almost 280,000 U.S. customers was exposed, including names, full/partial Social Security numbers, and (unauthorized access to) "protected" account-related data.

A $25M fine was levied, to boot.

According to the FCC's Enforcement Bureau, the fine is its largest ever for an information security or privacy concern and the enormous sum could conceivably be the biggest of its kind in the U.S.

The FCC has stated its intentions unequivocally: it is serious about enforcement of data privacy issues.

According to J. Trevor Hughes, president and CEO of the International Association of Privacy Professionals (IAPP), "We see a very active FCC with a clear goal."

Read on: http://www.scmagazine.com/att-fined-by-fcc-for-breaches-in-three-call-centers/article/408114/.

Survey Reveals Disconnect Between Perception and Use of Cyber Threats

A new report concludes that companies lacking cyber threat intelligence are at higher risk of succumbing to cyber attacks. Timely, up-to-the-minute, precise, and actionable data is critical to the effectiveness of a technology implementation.

The *Importance of Cyber Threat Intelligence to a Strong Security Posture*, a new report, details a dependence on threat intelligence as a practical solution to cybersecurity defense of critical infrastructure.

The study, commissioned by Webroot, and in partnership with the Ponemon Institute, expresses that most companies believe in threat intelligence as a constituent element of a fully developed cybersecurity defense, as it has a proven track record.

Here are some of the key findings from the research:

- Forty percent of the companies surveyed had a material security breach in the past twenty-four months.
  - Eighty percent suppose that if threat intelligence had been an integral part of their infrastructure at the time of the breach, the attack could have been averted, or the consequences minimized.
- Only thirty-six percent of the respondents rate their company's cyber defense as strong.
  - And so, current cyber defense practices are considered inadequate.
- Very nearly half of the respondents are increasing their arsenal of intelligence information in order to act against an attack or mitigate the consequences of one.

The new survey features perspectives from 693 IT and IT security professionals in the U.S. Sixty-one percent of the respondents are in the Fortune 1,000, Global 2000, and the Forbes List of the Largest Private Companies.

Continue reading: http://www.darkreading.com/vulnerabilities---threats/survey-reveals-disconnect-between-perception-and-use-of-cyber-threat-/d/d-id/1319796.

Dropbox Strikes Back Against Bartalex Macro Malware Phishers

Dropbox, a free file hosting service, has retaliated against a hacker group for illicitly using its cloud storage service to store and diffuse the Bartalex macro malware.

Christopher Talampas, a Trend Micro fraud analyst, apparently uncovered the campaign while he was investigating attacks aimed at the Automated Clearing House (ACH) electronic network for financial transactions in the United States.

In the end, Dropbox revoked the ability for accounts involved to share links.

Trend Micro revealed at least 1,000 malicious Dropbox links hosting the malware at the peak of the campaign.

For an in-depth study, read on: http://www.v3.co.uk/v3-uk/news/2406081/hackers-spreading-bartalex-macro-malware-with-phishing-attacks.

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.

Please note that henceforth, blog stories and excerpts will be located exclusively at the URL immediately above. So as to better share our expertise of threat models and attacks, we are merging this section of the *Threat Report* with *Threat Models*.

Threat Trends

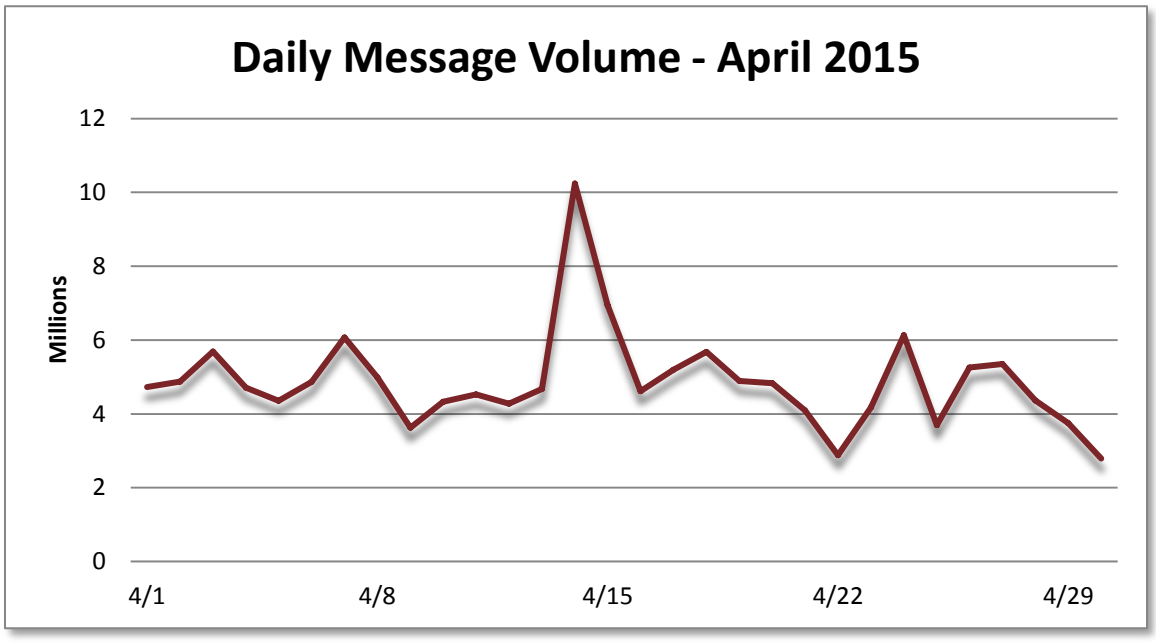
Spam Volume Trends

Proofpoint tracks spam volumes via a system of honeypots. The volumes historically track with that of our customer base.

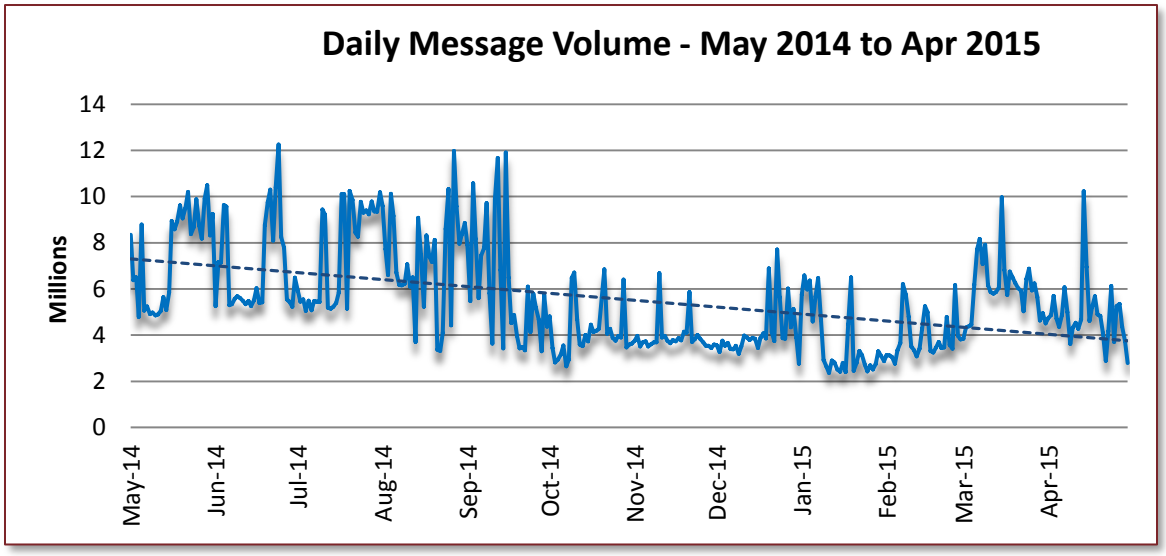
April's daily spam volume was a bit erratic, beginning decidedly above 4 million and fluctuating wildly between slightly above 6 million and just below 4 million for nearly the first two weeks of the month, the half-way point showed a burst of activity to 10 million.

Without any delay, the third week began with a plummet to very nearly 5 million. Following on the heels of the drama was nearly a mirror image of the first half of the month.

The month closed at roughly 3 million.



By comparison, March-over-April reflected a modest decrease in the volume of spam (19.46%). The year-over-year spam tally decreased by 36.60%.



Spam Sources by Region and Country

The EU clinched first place in April for the fifth consecutive month while the U.S. held on to second for the fourth consecutive month. China, meeting the challenge to move up through the hierarchy, captured third, and India maintained fourth for the second month in a row.

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

		Nov '14	Dec '14	Jan '15	Feb '15	Mar '15	Apr '15
Rank	1st	China	EU	EU	EU	EU	EU
	2nd	EU	China	US	US	US	US
	3rd	US	US	Vietnam	Vietnam	Russia	China
	4th	Russia	Russia	Argentina	Argentina	India	India
	5th	Argentina	Vietnam	China	Russia	China	TBD

The table below details the percentage of total spam volume for the March 2015 and April 2015 rankings noted above. The calculation for the EU is based on the inclusion of all member states, thereby producing a better representation of its volume. At 14.45%, the EU generated the majority of the world's spam. The remaining four countries in the top five slots were collectively responsible for 18.34%—above the output of the EU.

March 2015			April 2015		
1	EU	30.89%	**1**	EU	14.45%
2	US	9.75%	**2**	US	10.45%
3	Russia	5.24%	**3**	China	6.73%
4	India	4.97%	**4**	India	1.16%
5	China	3.06%	**5**	TBD	TBD

The following table displays the top five spam-sending member states of the European Union (EU) for March 2015 and April 2015, in addition to the percentage of total spam volume for each country.

March 2015			April 2015		
1	France	3.56%	**1**	Italy	1.09%
2	Italy	3.28%	**2**	Netherlands	0.84%
3	Germany	3.19%	**3**	UK	0.49%
4	Spain	2.54%	**4**	Germany	0.44%
5	UK	1.62%	**5**	Czechoslovakia	0.43%

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

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

