proofpoint

Proofpoint Threat Report

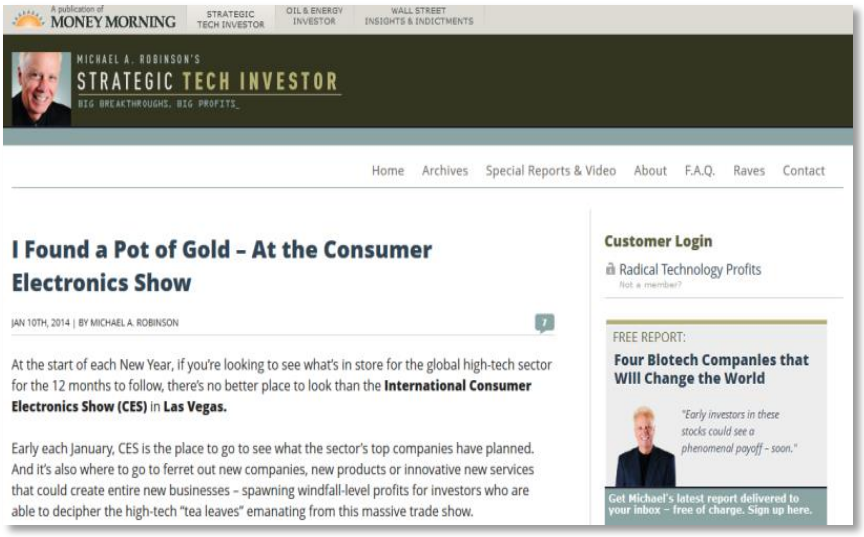
December 2013

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

Threat Models

Beware Investing Advice Bearing Unwanted Returns

The turn of each year brings the requiste summations of the past year and predictions for the coming one. Financial advisors are excellent soothsayers, or at least claim to be. Beware those newsletters and sites bearing malicious code, something akin to coal in the stocking of old. Proofpoint researchers uncovered an infection of the well known Strategic Tech Investor site. This is a classic watering hole attack. Elements include a community of shared interest, use of a trusted content source - a legitimate, reputable site and a newsletter used to lure visitors. "Relying on



websites the group trusts makes this strategy efficient even with groups that are resistant to spear phishing and other forms of phishing.[1]"

Another interesting note about this attack is the use of an exploit kit. Since the arrest of the alleged author of Black Hole, we've seen a shift away from exploit kits to other attack mechanisms i.e. use of Dropbox. This attack in particular utilized the Styx exploit kit. Three tell-tale characteristics fingerprint Styx. The first is long URL paths which include random characters and numbers. These are followed by java exploits. Finally, the use of trailing parameters mimics the same random character string as the exploit. Each of these is highlighted in Figure 2.

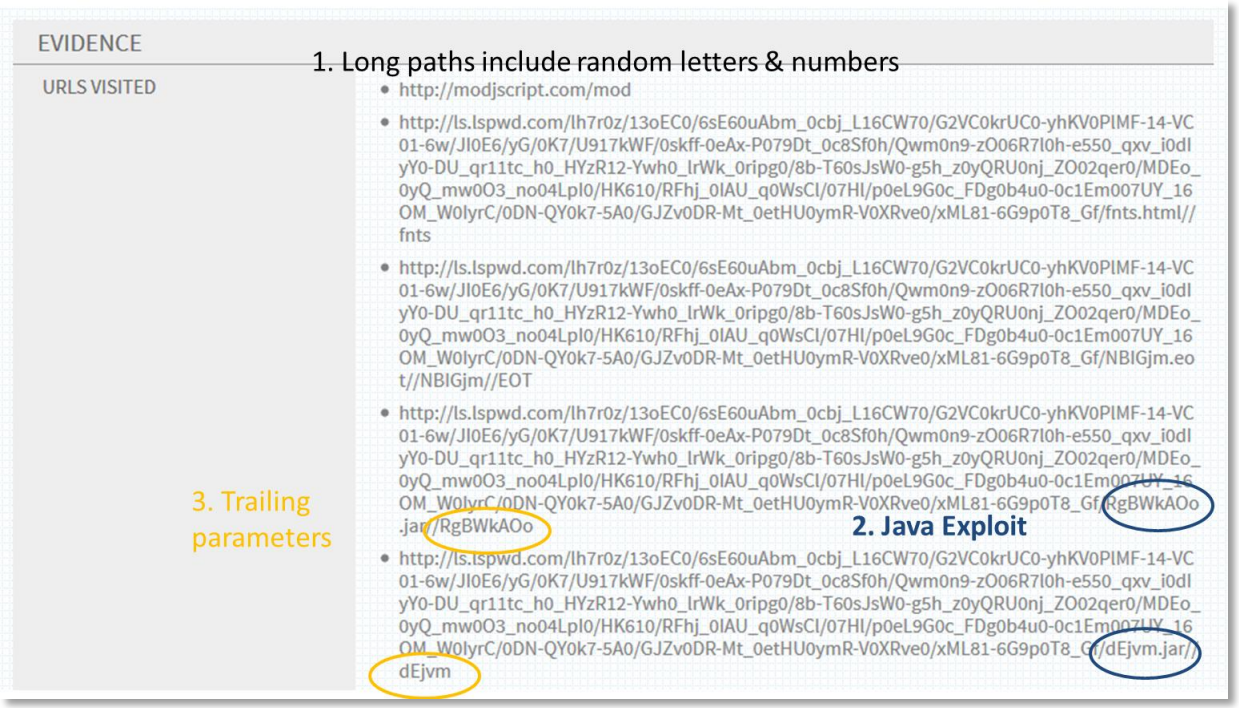
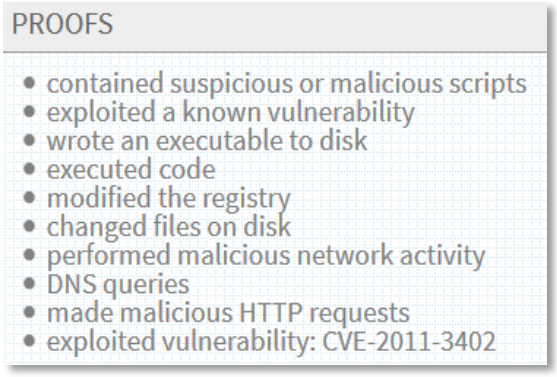


Figure 2: Styx Exploit Kit Characteristics

A closer look at the forsencis provided by Proofpoint's Dynamic Malware Analysis Service, Styx utilized a known vulnerability – CVE-2011-3402. Mitre.org describes this CVE as an "Unspecified vulnerability in the TrueType font parsing engine in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1, allows remote attackers to execute arbitrary code via crafted font data in a Word



[1] Wikipedia reference: http://en.wikipedia.org/wiki/Watering_Hole

document or web page, as exploited in the wild in November 2011 by Duqu, aka "TrueType Font Parsing Vulnerability.[2]"

Figure 4 reveals the TrueType Font vulnerability used.

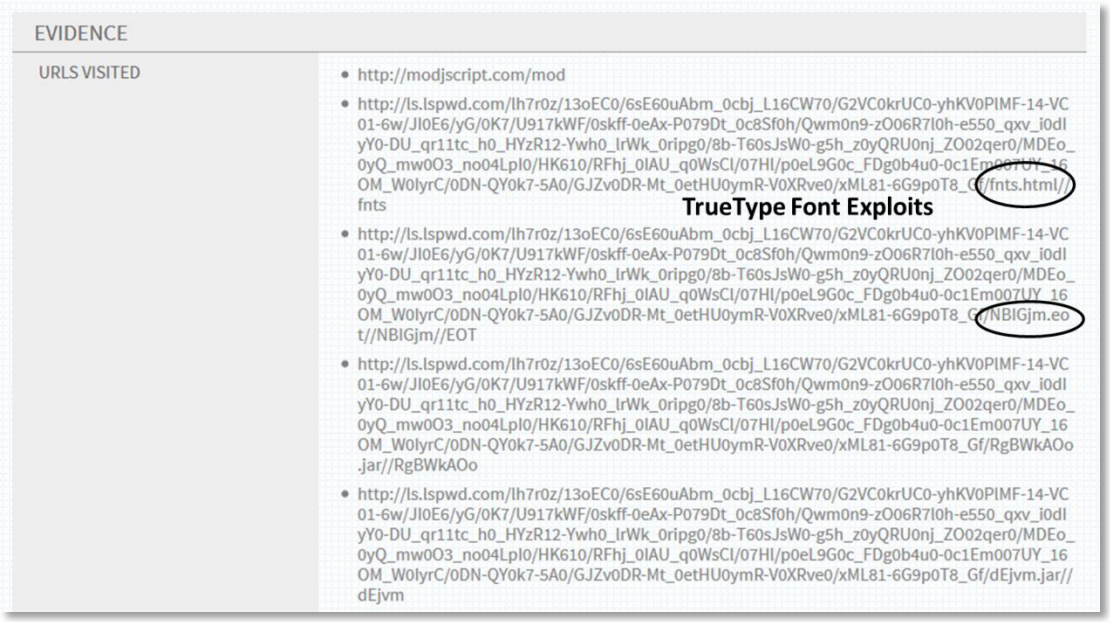


Figure 4: TrueType Font Exploits

The first reference in Figure 4 point to fnts.html, evident from the name, it references a font store. The .eot extension included in the second refers to Embedded Open Type (EOT) fonts. These "are a compact form of OpenType fonts designed by Microsoft for use as embedded fonts on web pages.[3]"

Once the target machine was exploited, the attack continued by downloading and executing a payload. The executables utilized the same random character naming scheme as in the URL naming. Figure 5 highlights the downloaded executables.

Figure 5: Executables

[2] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3402
[3] http://en.wikipedia.org/wiki/Embedded_OpenType

With the machine infected, the malware attempts to call back to the Command & Control (C&C) servers. DNS queries and network activity reveal the detail in Figure 6.

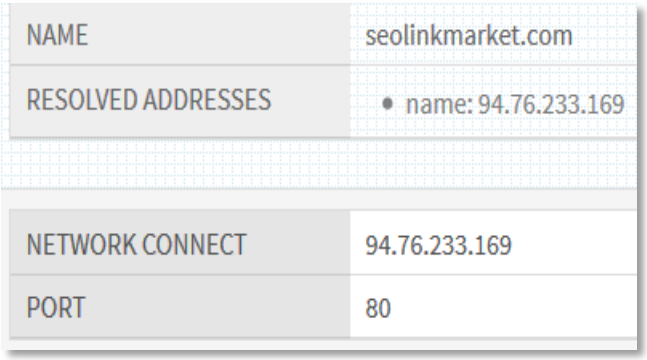


Figure 6: DNS and Network Activity

Seolinkmarket.com and the associated IP address have been linked to the Fareit/Tepfer malware. Microsoft calls it PWS:Win32/Fareit.gen!I and describes it as "This password stealing trojan gathers sensitive information such as your login and password details and sends them to a remote attacker. It can also download other malware, including variants of PWS:Win32/Zbot, which can give an attacker control of your computer.[4]" PWS:Win32/Zbot is also known as Zeus, the widespread trojan used to steal banking credentials. One malware infection begets another, leads to another, then another variant or one with another goal.

Dynamic malware analysis tools such as cloud based sandboxing provide key forensic insight into the multiple levels and complexity of an attack. They also help humans keep pace with the ever changing threat landscape. Lack of malware instances and forensic evidence portends the decline of one malware or family, for example. Furthermore, when a large malware variant or player is removed from the landscape, cloud-based sandboxing similar to the technology used in Proofpoint's Dynamic Malware Analysis Service, provide key insight for researchers to the heretofore unknown threats that fill the gap.

Threat News

Experian: More Healthcare data breaches in 2014

InformationWeek states that, according to a recent report by Experian, 2014 will be a rough year of data breaches for the healthcare industry. The *2014 Data Breach Industry Forecast* states, "The healthcare industry, by far, will be the most susceptible to publicly disclosed and widely scrutinized data breaches in 2014," Industry size and the new Healthcare Insurance Exchanges combine to provide a large attack vector, according to the report. Full HIPPA/HITECH rules mature to full enforcement in 2014. These stronger regulations could result in record fines. The full story is located here: http://www.informationweek.com/healthcare/policy-and-regulation/healthcare-data-breaches-to-surge-in-2014/d/d-id/1113259

[4] http://www.microsoft.com/security/portal/threat/encyclopedia/Entry.aspx?Name=PWS%3AWin32%2FFareit.gen!I

Hackers Using the Spoils from Adobe Breach

A phishing campaign claiming to deliver Adobe license keys is underway Abode warned in a blog post. It encourages users to delete suspicious messages and not to be tempted by attachments or hyperlinks. Adobe blog post; http://blogs.adobe.com/psirt/?p=1035

Threatpost.com provides a fuller description and example message text. Their blog post can be read here; http://threatpost.com/adobe-warns-of-new-license-key-scam-phishing-campaign/103278

93% of Large UK Business suffered a Breach in 2013

93% of large companies, according to a survey commissioned by the UK Government's Department for Business, Innovation and Skills (BIS) experienced a breach in 2013. Smaller companies were breached at 87%, up from 76% in 2012. Attacks and breaches are costing UK companies across all sectors. "The worst security breaches are currently costing large companies an average of £450,000 to £850,000 each, while smaller businesses typically experienced losses of between £35,000 and £65,000." The full story is located here; http://www.itproportal.com/2013/12/16/93-of-organisations-suffered-a-data-breach-in-2013/

Threat Insight Blog

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

5 Attackers & Counting: Dissecting the "docx.image" Exploit Kit

The recent CVE-2013-3906 zeroday document exploit utilizes multiple new techniques and has been observed in the work of at least five different attacker groups. Judging by the fast adoption rate of this exploit by attackers, we believe the framework will provide a common template for future MS Office document exploits.

A few vendors have independently published posts on different incidents involving this exploit, but a collective study on the exploit framework itself, how it has been used, and by whom has not been produced until now. This post aggregates all this information.

Full post is found here; http://www.proofpoint.com/threatinsight/posts/dissecting-docx-image-exploit-kit-cve-exploitation.php

Attackers using the guise of "Fraud Prevention" to… well, commit fraud!

Last week we saw the return of an attacker group that frequently used lures involving the American Express brand. We call this group the "index.html" group internally at Proofpoint as they always use URL-based attacks, where the URL contains a random English dictionary word and ends in *index.html*. This group used the Blackhole exploit kit almost exclusively for their attacks before Paunch's arrest, but after taking a hiatus they now seem to be back and have shifted gears to credential phishing.

Full details are here; http://www.proofpoint.com/threatinsight/posts/attackers-using-the-guise-of-fraud-prevention.php

Attackers making malware delivery more secure

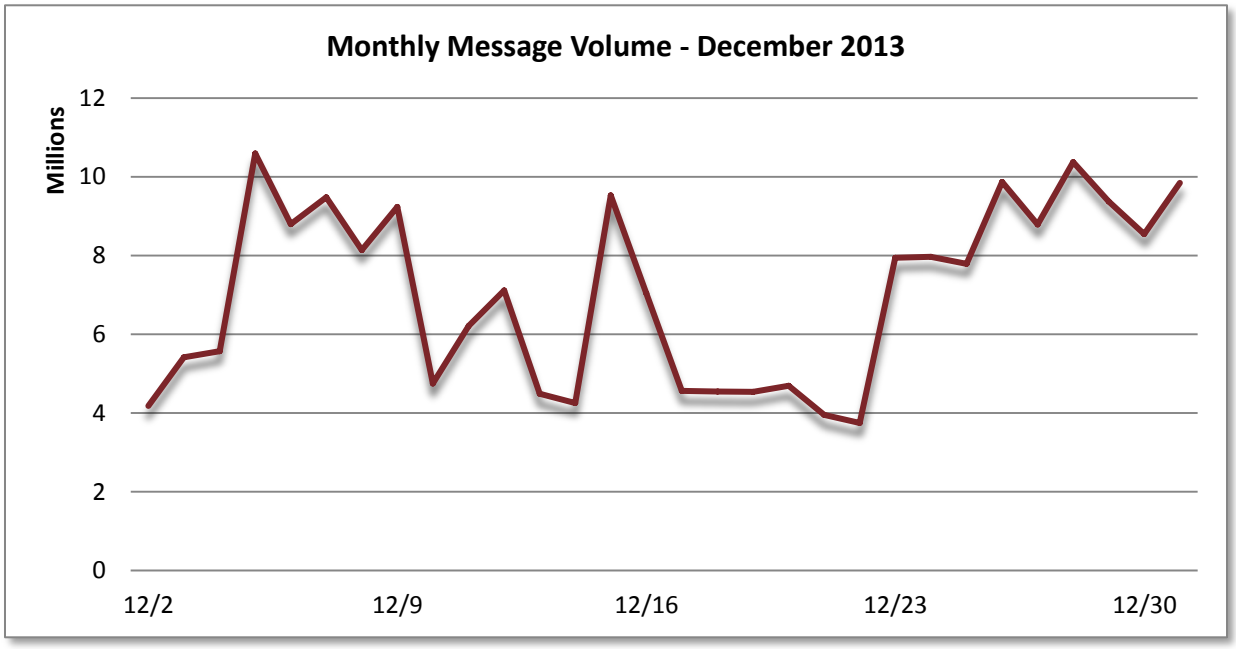
We've recently observed an uptick in targeted phishing emails using SSL in their attacks. This is different than earlier reports of how Trojans like "Gameover" are using encrypted SSL connections to fetch malicious payloads. Rather, we are seeing attackers directly send SSL-protected URLs in targeted phishing emails that link to their malware which is almost always packed inside a zip file. The expectation is that some of the recipients who click on the link will open the zip file. While this approach certainly has a lower infection rate than typical drive-by download attacks, it does have the benefit of requiring none of the complex infrastructure required for a successful exploit kit campaign.

The full post can be found at; http://www.proofpoint.com/threatinsight/posts/attackers-making-malware-delivery-more-secure.php

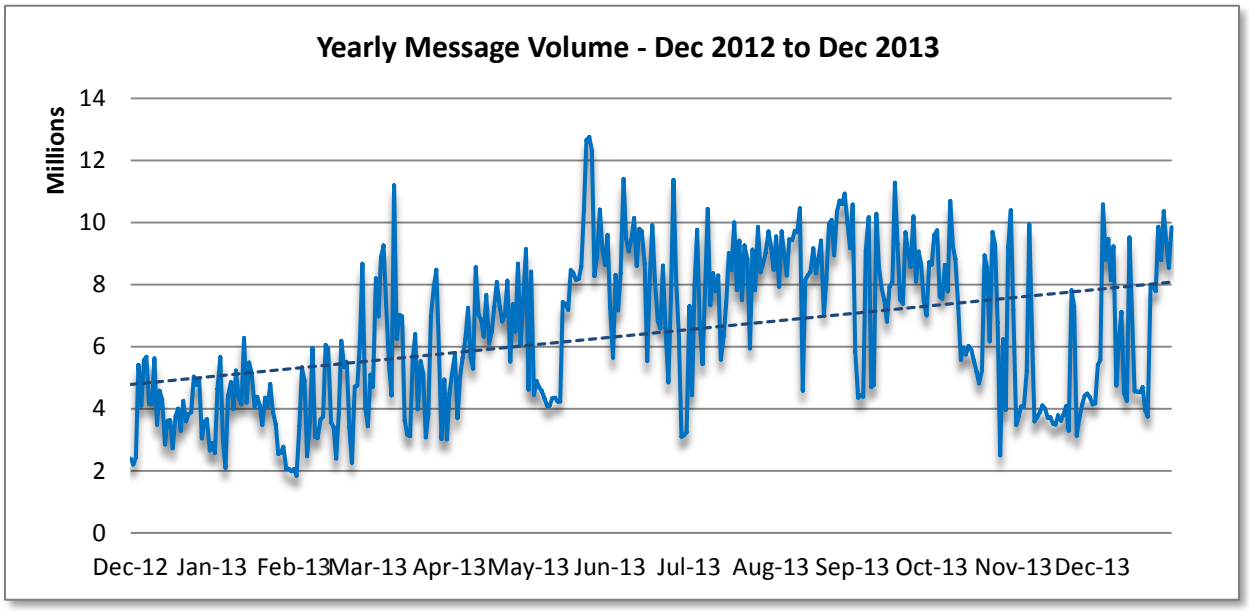
Threat Trends

Spam Volume Trends

Proofpoint tracks spam volumes via a system of honeypots. The volumes historically track with that of our customer base. In December daily spam volumes recovered lost ground in November. Volumes were erratic the entire month. They vacillated in a wide range from below 4 million messages/day and reached heights of 10 million several times. Volumes peaked at the beginning of the month, dipped around the 10th but spiked again in mid-month. Spammers took an early break as volumes dropped prior to the holidays, yet returned with a strong showing to end the month with three days near 10 million daily volumes.



Spam volumes returned to a robust pattern in December. Average month over month volumes increased 53.25% in December. This month also saw a record 75.88% year over year increase. Spam volumes have increased 16.90% in the 2013 calendar year. Even with the hackers getting all the press, spammers are alive and well.



Spam Sources by Country

A couple usual suspects returned to the Top 5 spam sources in December. The European Union continues its notorious reign as the number one spam generating region in the world. The US returned to its customary number two position. China lost a slot to land at third. Argentina regained the fourth ranking. India retained the fifth spot. The following table shows the Top 5 spam sending countries for the last six months.

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

The table below details the percentage of total spam volume for each of the above rankings. The European Union increased its volume output by 17.78% and continues to generate most of the world's spam. China's output fell in line with the others on a percentage basis, recording 5.27% output.

November 2013			December 2013		
1	EU	13.97%	1	EU	16.99%
2	China	12.22%	**2**	US	6.34%
3	US	7.26%	**3**	China	5.27%
4	Japan	3.37%	**4**	Argentina	4.46%
5	India	3.33%	**5**	India	3.41%

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