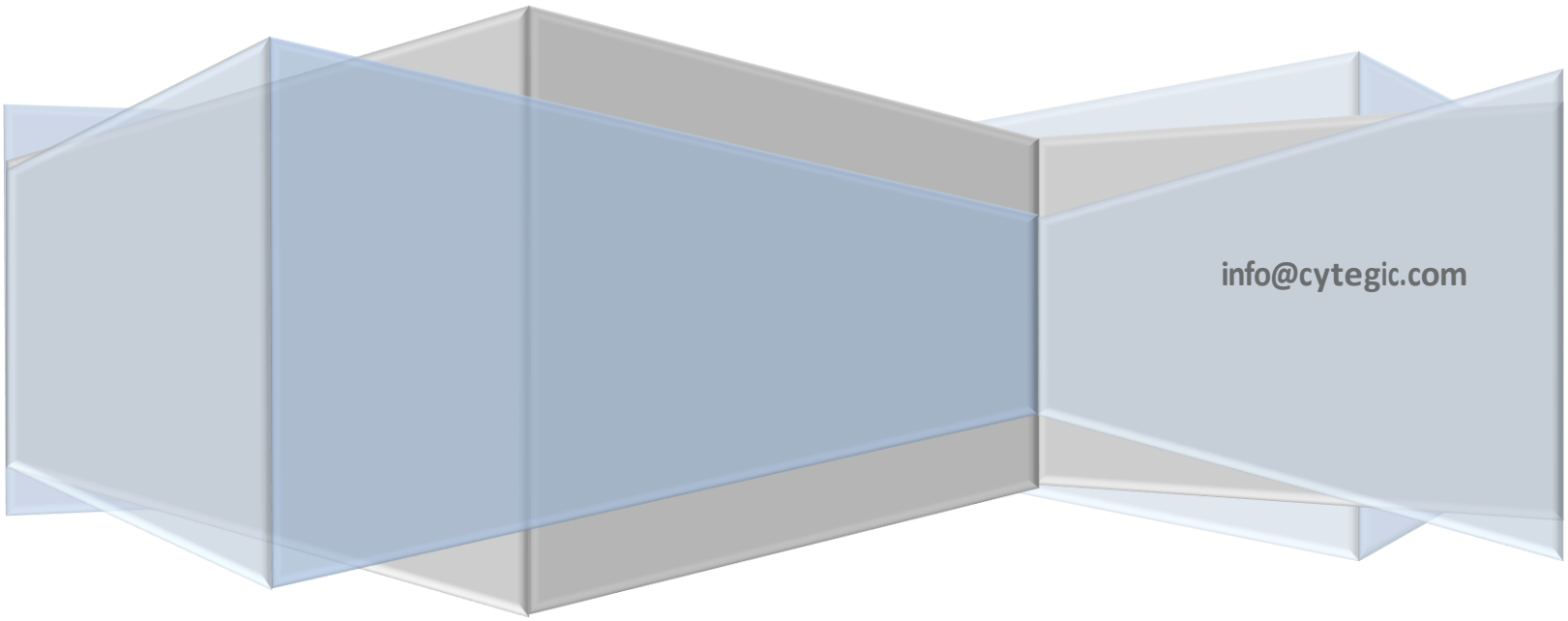
cytegic

DyTA Intelligence Update

November 2015



info@cytegic.com

November 2015 - Cytegic DyTA Intelligence Update

Holiday Season 2015

Intro

Cytegic DyTA intelligence platform gathers, processes and analyses hundreds of thousands of intelligence feeds on a month basis, to allow a quick and understandable cyber-trend analysis. DyTA enables cyber-intelligence analysts and CISOs to understand and analyze the threat level of each attacker and attack method relevant to their organization, according to their geo-political region, industry sector and corporate assets.

The following report represents the most interesting and active cyber-trends that DyTA analyzed before and during previous holiday seasons in USA and a forecast for the coming holiday season. As a background we analyzed the main trends that occurred during the years 2012-2014, during the same period.

The most noticeable trend we observed is that hackers focus, during the holidays, on the special sale days throughout the network such as "Black-Friday", Cyber-Monday, "New Year sales" and etc.

Executive Summary

- The most active cyber-attackers during the holiday season against US retailers are financially-motivated attackers, followed by politically-motivated ones. In 2014's holiday season, financial hackers accounted for more than a third of the overall attacks and we forecast them to be more than half of this season's threat landscape.
- The top TTPs in the holiday season are forecasted to be Malware, Email Social-Engineering, Denial of Service and Terminal Malware, similar to previous years when financial hackers targeted large retailers in order to steal payment card information and client data.
- The most targeted assets in this period are forecasted to be Payment Card information, Client Data, Cash and Financial Transactions.
- Attacks against retailers usually take place a few days before a major holiday, with the week before Christmas being the most threatened time in this period
- Retailers, and in that sense any company who processes payments and financial transactions, should be on the highest alert level during the coming weeks and prepare in advance towards the specific attack methods which are going to targeted their assets, as mentioned above.

Top trends

1. Earlier Years Threat Landscape

When analyzing previous holiday seasons, during the years 2012-2014, we identified several interesting trends:

a. A recent survey[1] showed that the average cost of cybercrime for US retail stores more than doubled from 2013 to an annual average of $8.6 million per company in 2014. The annual average cost per company of successful cyber-attacks increased to $20.8 million in financial services, $14.5 million in the technology sector, and $12.7 million in communications industries.

b. During the holiday season, cyber-attacks are more prominent surrounding special sales days, such as "Black-Friday", Cyber-Monday, "New Year's sales", etc. The most targeted assets in these attacks are Payment Credentials, which consist mostly of PIN numbers, usernames and phone numbers of paying customers.

c. The mobile traffic during holidays increases in about 45%[2] and research shows that 53% of scanned websites contained unpatched and potentially exploitable vulnerabilities. The page views in this period are between 9-11 million per minute[3] and retail experts calculated that shopping spending in 2014 reached over $600 billion yearly with $105 billion just during the holiday season, a 4% growth from 2013, which out of that 8-11% are online sales[4].

d. Cyber-attack traffic is five times higher during "Black Friday" than in the beginning of November.

e. The most common TTP on retail web apps are malicious requests, that fall into three main categories: SQL injections, DDoS attacks, and image/cross-site scripting[5] (SQL injections happen twice as much than any other method). On top of that, there is a heightened activity of Botnents and mobile app store frauds.

f. Different researches saw an average of 547 attacks per day during the holiday season, where a month earlier the average is 150 attacks per day and 267 in the month that follows[6].

[1] http://www.heritage.org/research/reports/2014/10/cyber-attacks-on-us-companies-in-2014
[2] http://payments.cardinalcommerce.com/cyber-criminals-try-to-dampen-the-holiday-spirit
[3] http://payments.cardinalcommerce.com/cyber-criminals-try-to-dampen-the-holiday-spirit
[4] https://nrf.com/media/press-releases/optimism-shines-national-retail-federation-forecasts-holiday-sales-increase-41
[5] http://payments.cardinalcommerce.com/cyber-criminals-try-to-dampen-the-holiday-spirit
[6] http://www.securityweek.com/cybercriminals-gear-holiday-shopping-season

g. For retailers, threats typically arise from competitors, angry users, financial hackers looking for financial gain and hacktivists who associate certain retailers with specific causes[7].

h. The potential losses of an e-commerce site going down - even for just 15 minutes - on Black Friday or Cyber Monday can reach $8000 a minute, which means $500K per hour[8].

i. A recent poll found that 69% of respondents were concerned about having their credit card information stolen from stores, and 62% were worried about having their computer or smartphone hacked. However, a recent survey of 1,000 consumers found that while nearly 50% were victims of a data breach, 45% have not changed their shopping behavior when using credit and debit cards.

j. The most severe and interesting cyber-attack that occurred in the last years was the attack on huge American retailer "Target" on Thanksgiving of 2013. Sensitive information of as many as 70 million credit and debit card were stolen, including card numbers, telephone numbers, emails and addresses. The targeted attack started on "Black-Friday" and lasted until December 15th, using a very sophisticated attack method – piggybacking the HVAC vendor's system to get through to Target's network and then spreading a "fresh from the market" POS malware throughout the POS terminals.

[7] http://www.retailtouchpoints.com/features/executive-viewpoints/the-holiday-selling-season-a-hacker-s-ideal-time-for-attack

[8] http://www.retailtouchpoints.com/features/executive-viewpoints/the-holiday-selling-season-a-hacker-s-ideal-time-for-attack

Threat landscape in 2014 and Forecast for 2015

When observing the holidays timeframe 11/01/14-01/06/15, first it's important to be aware of the specific dates:

- Thanksgiving - November 27th
- Black Friday - November 28th
- Cyber Monday - December 1st
- Christmas - December 25th
- New Year's Eve - January 1st

From the analysis we made using our DyTA Intelligence Platform, we identified the following trends and patterns:

- **The top attackers in this timeframe are financial hackers** (38.2% of all attacks), which matches the information we gathered mentioned above.
- **Attacks against retailers usually take place a few days before a holiday** (the peaks in the graphs below).
- An important note about the 2014 chart is that the high numbers of attacks of political cyber-warrior (36.2% of all attacks) in the middle of December 2014 can be attributed to the "cyber war" between North-Korea and Sony Pictures Entertainment[9] which started at the end of November and continued throughout December[10].
- From observing the charts below of 2014 and 2015 with the forecast, we can see that **the two main types of attackers - Financial Hackers and Politically-motivated attackers - stay on top**, and seem to be the most threatening concern this season as well. **The week before Christmas is when retailers should be on their most heightened alert level, with Thanksgiving coming in second.**

[9] http://blogs.cfr.org/cyber/2014/12/19/cyber-week-in-review-december-19-2014/
[10] https://www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-december-2014-sony-hack/

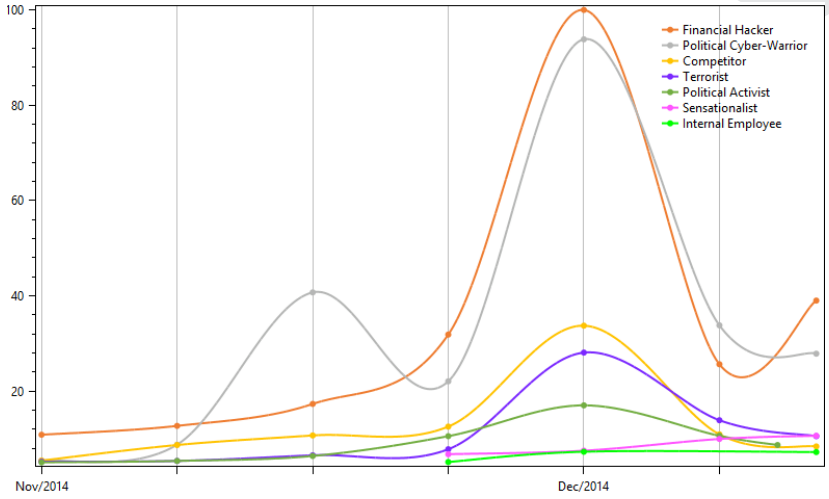


Chart 1: 2014 analysis of attackers types by weeks

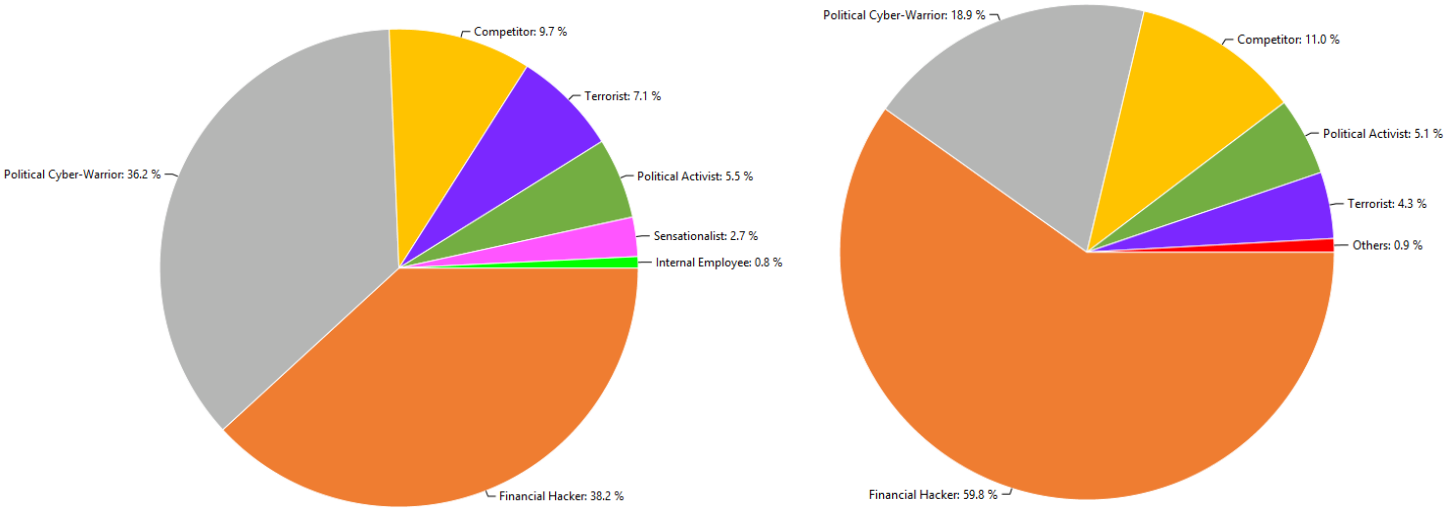


Chart 2: 2014 statistics (left) and 2015 statistics (right) of attackers types

When looking from the perspective of TTPs, it is clear to see that the main methods used were Malware (41.4%), terminal malware (16.8%), E-Mail Social Engineering (12.8%), and Denial of Service (8.5%). This data matches the background we mentioned above.

The forecast generated by DyTA for this year's holiday season shows an interesting change from last year – while the top TTPs remain the same and Malware is still forecasted to be the top TTP, terminal malware took a step back and in its place are forecasted to be email social engineering attacks.

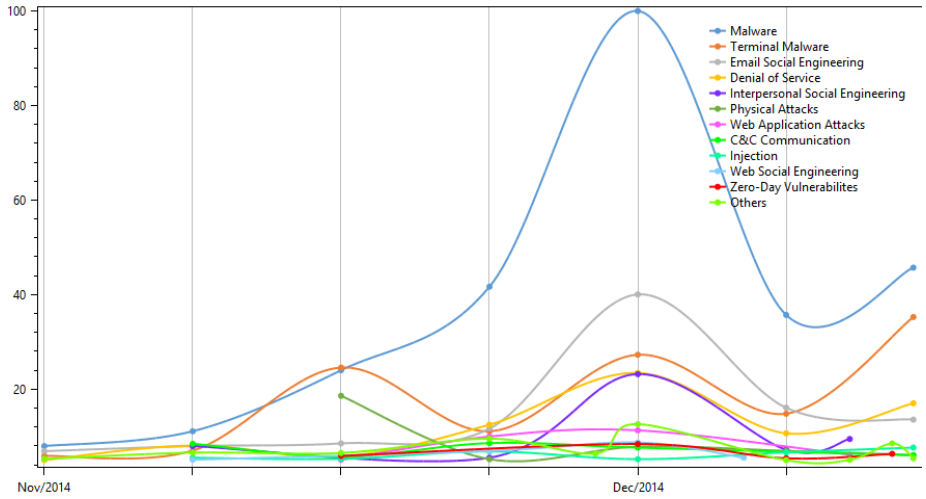


Chart 3: 2014 analysis of TTP by weeks

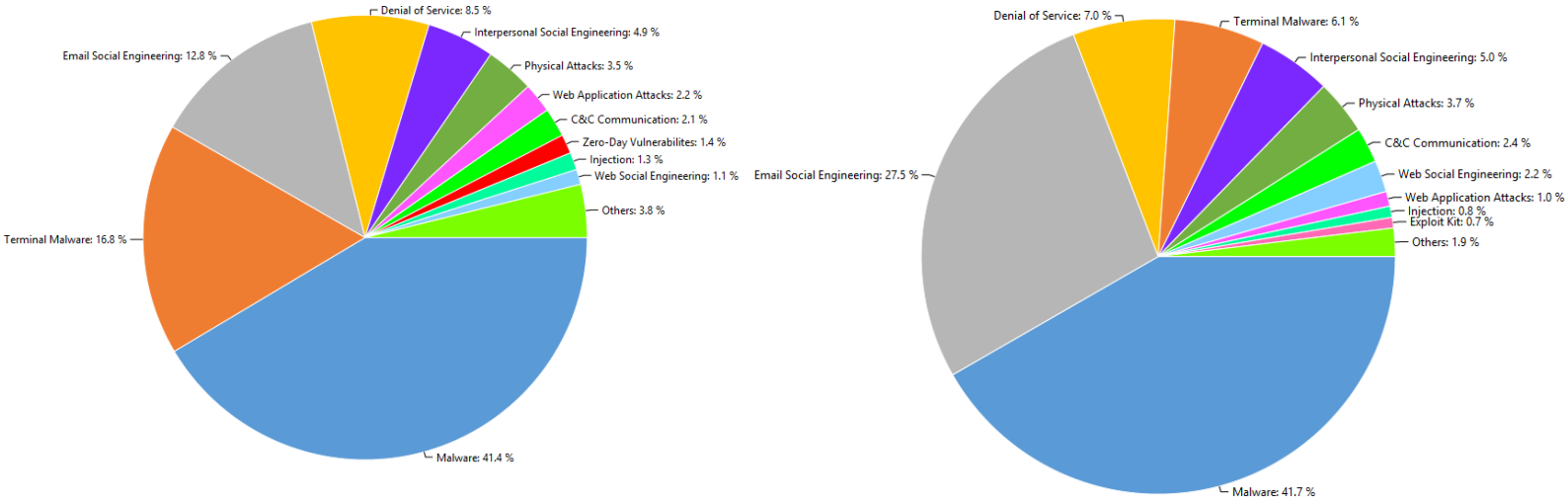


Chart 4: 2014 statistics (left) and 2015 statistics and forecast (right) of TTP

According to the data gathered and analyzed using DyTA the most targeted assets in last year's attacks on US retailers during the holiday season were Payment Cards, Client Data, Financial Transactions and Services to Clients. This coincides with the prominence that financially motivated have this time of the year on the threat landscape.

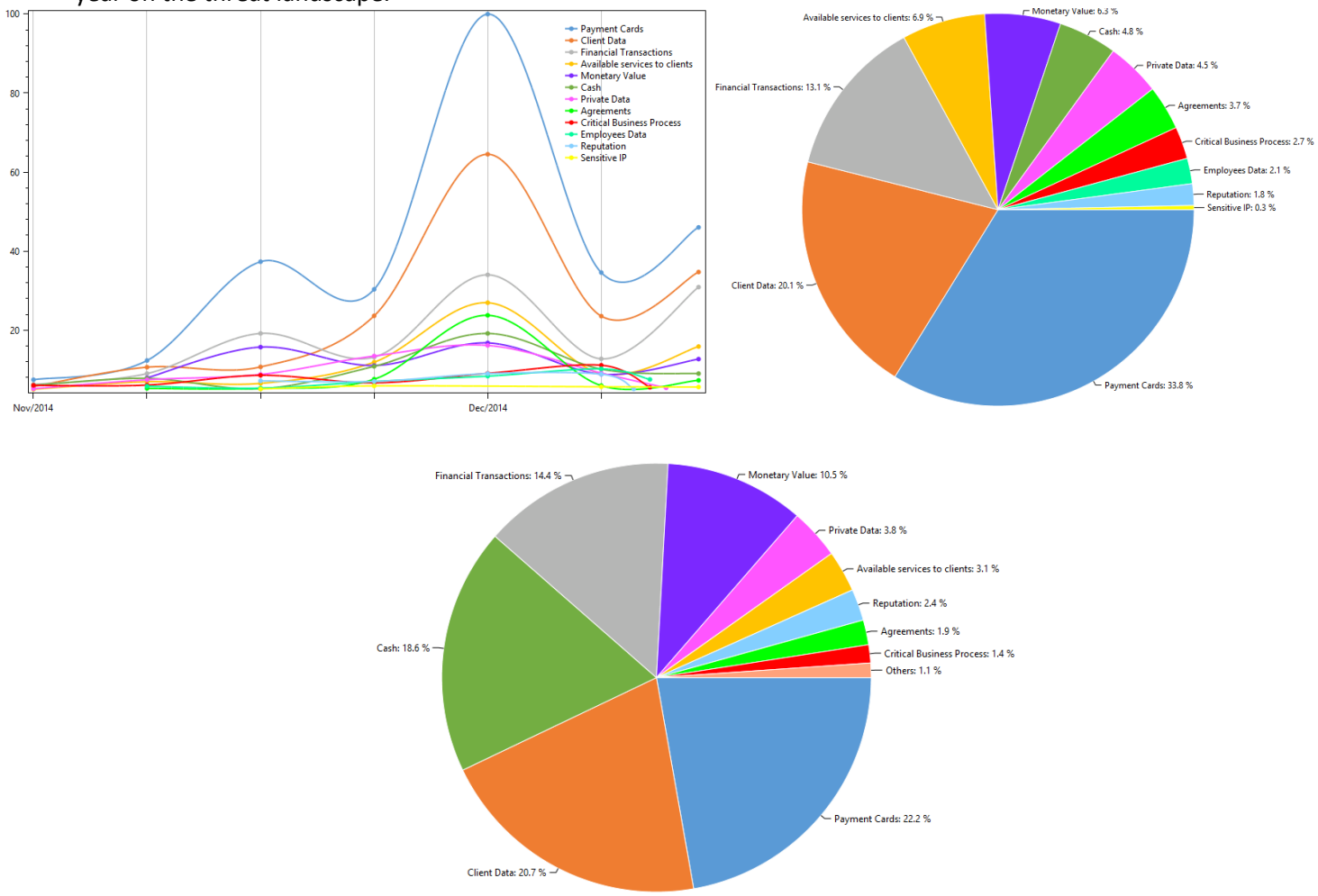


Chart 5: targeted assets - 2014 analysis (top left) and 2014 statistics (top right); 2015 statistics and forecast (bottom)

Another interesting trend we saw from looking at the statistics is that from an Industry perspective there were two peaks at the holidays of 2014. The first was at the second part of November and another also at the second part of December.

In November 2014 the main targeted industries were government, banking and finance, retail and media. We identified a rise at retail starting at the end of November with Thanksgiving. The main industries which last year suffered great loses, will probably confront the same issues this holiday season.

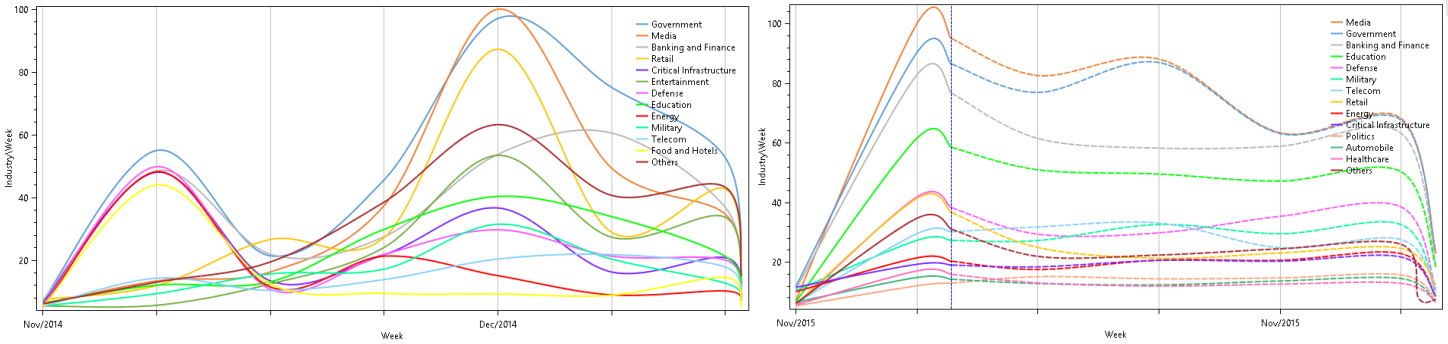


Chart 6: 2014 analysis (left) and 2015 analysis and forecast (right) of industries by weeks

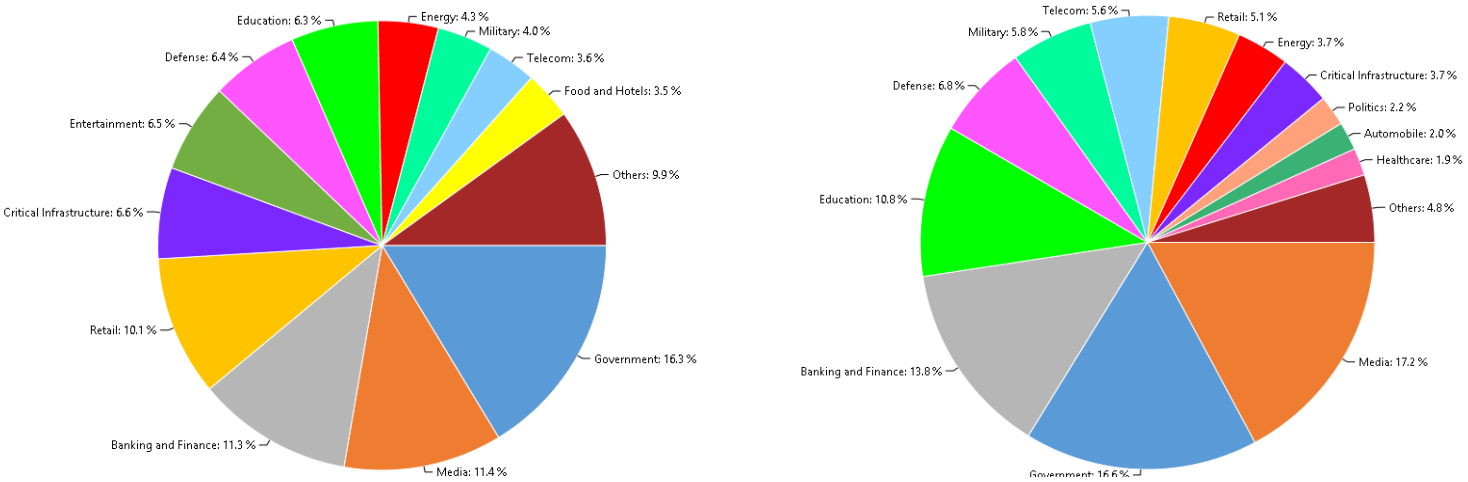


Chart 7: 2014 statistics (left) and 2015 statistics (right) of industries