Comparing Alternatives to Measure the Impact of DDoS Attack Announcements on Target Stock Prices

Abhishta*, Reinoud Joosten, and Lambert J.M. Nieuwenhuis
University of Twente, Enschede, The Netherlands
{s.abhishta, r.a.m.g.joosten, l.j.m.nieuwenhuis}@utwente.nl

Abstract

Distributed denial of service (DDoS) attacks are responsible for creating unavailability of online resources. Botnets based on internet of things (IOT) devices are now being used to conduct DDoS attacks. The estimation of direct and indirect economic damages caused by these attacks is a complex problem. In this article we analyze the impact of 45 different DDoS attack announcements on victim firm's stock prices using three different approaches and compare the results. We show that the assumption of cumulative abnormal returns being normally distributed leads to overestimation/underestimation of the impact. We solve this problem by using an empirical distribution of cumulative abnormal returns for hypothesis testing. Finally, we demonstrate the impact of DDoS attack announcements in each of the cases.

Keywords: DDoS attacks, stock market study, event study, economic impact.

1 Introduction and Background

Distributed denial of service (DDoS) attacks are responsible for creating unavailability of online resources which can lead to both direct and indirect losses [1]. In 2016 the intensity of DDoS attacks peaked at 1.4 Tb/s. The biggest DDoS attack targeted the systems operated by domain name service (DNS) provider Dyn [2]. A few months later this firm was bought by Oracle [3]. One can only speculate about the change in the valuation of the firm as it is not publicly traded. In this study we investigate the impact of DDoS attack announcements on the stock prices of the victim firms.

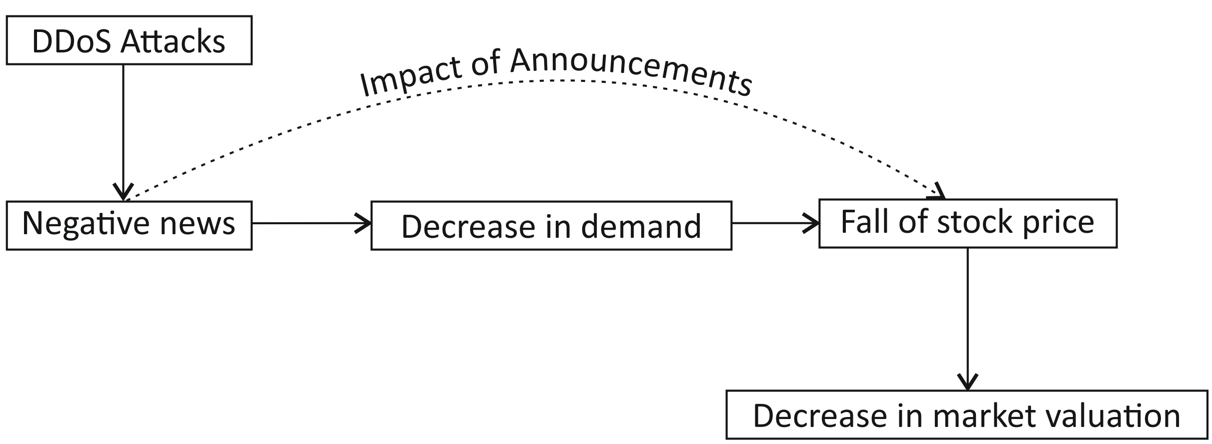


Figure 1: Impact of a DDoS attack announcement on market valuation of the firm

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 8:4 (December), pp. 1-18

*Corresponding author: University of Twente Enschede, The Netherlands 7522-NH, Tel: +31-(0)65-232-5152, Web: http://www.abhishta.xyz/

The stock price of a firm is representative of its market value. In the past economists have analyzed the impact of an economic event on the value of the firm [4]. A strategic business decision e.g. *merger or an acquisition* can impact the future dividends significantly. For instance, in the case of an expected negative impact on the future cash flows, so investors may choose to sell the shares and invest in a different stock.

DDoS attacks may lead to negative news articles about the firm. These news articles come as a negative sentiment shock and can negatively influence the demand of the victim firm's shares, this in-turn leads to the fall of stock prices of the attacked company [5]. Figure 1 shows the conceptual relationship between DDoS attack events and decrease in market valuation of the victim firm. It also shows the empirical link that we investigate in this article.

Estimating the impact of cyber security related events is a complex problem [6, 7]. Several studies have tried to investigate the impact of cyber security related announcements on the victim stock prices and we discuss the results and limitations of these studies in Section 2. In this article we use three different methods for analyzing the impact of these attack announcements on target stock prices and then discuss and explain the differences in results.

This is an extended version of our study [8] that analyzed the impact of DDoS attack announcements on victim stock prices. In this article we compare the method proposed in [8] with the traditional method of event studies and illustrate the disadvantages of using the assumptions and approximations considered in those. We also analyze an extended set of DDoS attack announcements and re-emphasize the results of our previous study.

2 Related Literature

Event studies have been used by researchers to study the impact of various firm related announcements on the stock price. Mackinlay [4] discussed a method of conducting an event study including various market estimation models. In this section we discuss articles that have contributed to evaluation of the impact that cyber security event announcements have on victims' stock prices.

Hovav and D'Arcy [9] used a so-called one-factor market model in order to estimate stock prices. Equation 1 shows the estimation model used by them, where r_{it} represents the return rate of the stock i on day t and r_{mt} represents the rate of return of the market index on day t. As an example, r_{it} can be computed as $(P_{it} - P_{it-1})/P_{it-1}$, where P_{it} is the price of the stock on day t. The parameters α_i and β_i are firm dependent coefficients and can be estimated using ordinary least squares (OLS). The stochastic variable ε_{it} is the error term with $\mathbb{E}[\varepsilon_{it}] = 0$. Hovav and D'Arcy [9] analyzed a sample of 23 announcements of denial of service attacks and were not able to find any significant impact of these announcements on the concerned stocks.

$$r_{it} = \alpha_i + \beta_i r_{mt} + \varepsilon_{it} \tag{1}$$

Later, Campbell et al. [10] used the estimation model shown by Equation 1 to analyze a sample of 43 announcements of all kinds of cyber attacks. They calculated the abnormal returns by using Equation 2. Further, they calculated cumulative abnormal returns (*CAR*) by using Equation 3. They assumed these *CAR*s to be normally distributed and used a Z-statistic to test their hypothesis (i.e. there was no impact of cyber attack announcements on victim stock prices) and reported significant negative impact due to information security breach announcements.

$$AR_{it} = r_{it} - (\hat{\alpha}_i + \hat{\beta}_i r_{mt}) \tag{2}$$

$$CAR_n = \sum_{t=-1}^{n} AR_{it} \tag{3}$$

Cavusoglu et al. [11] and Kannan et al. [12] also used the above described method for analyzing the impact of security breach announcements. The former concluded that these announcements not only influence the value of the announcing firms but also the value of their internet security developers. While the latter considered a sample of 102 and reported a decrease of 1.4% in the market valuation relative to the control group.

Gordon et al. [13] used a so-called three factor Fama-French model [14] for the estimation. This model estimates the stock price on the basis of company size, company price-to-book ratio, and market risk, and can be mathematically represented as shown by Equation 4. SMB_t is the difference between the return on the portfolio of small stocks and the return on the portfolio of large stocks on day t, and HML_t is the difference between the return on a portfolio of low-book-to-market stocks and the return on a portfolio of low-book-to-market stocks on day t. The parameters a_i,b_i,s_i and h_i are Fama and French three-factor model estimated firm-dependent coefficients. The stochastic variable ε_{it} is the error term with $\mathbb{E}[\varepsilon_{it}] = 0$. [13] reported no significant impact due to post 9/11 announcements.

$$r_{it} = a_i + b_i r_{mt} + s_i SMB_t + h_i HML_t + \varepsilon_{it} \tag{4}$$

These mixed results motivate us to evaluate the impact of the choice of model and the underlying assumptions in the study on the final results. Thus, in this article we evaluate the impact of DDoS attack announcements on victim stock prices using three different methods and compare their results in Section 4. Section 3 discusses the our methodology.

3 Methodology

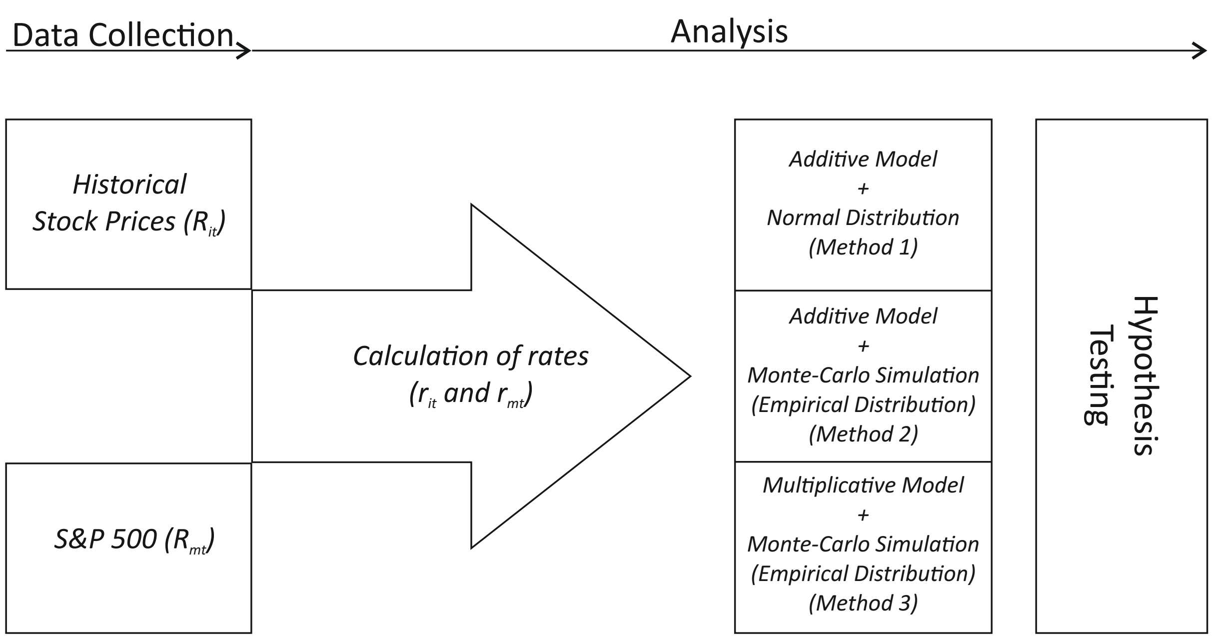


Figure 2: Methodology for this study.

The methodology used by us can be broadly subdivided in two parts:

1. Data Collection
2. Analysis

We analyze the impact on stock returns using three different methods. Firstly, we use the event study method employed by many of the previous articles [10, 9, 11]. In the second method, we use an additive market model for the estimation of return rates and then use the empirical distribution of abnormal returns by generating random scenarios for analyzing the additive cumulative abnormal return. In the last method we use the method proposed by us, that makes use of a multiplicative model for estimation and later uses multiplicative cumulative abnormal returns for analysis [8]. Figure 2 illustrates the step by step process used.

3.1 Data Collection

The data set in this study consists of all DDoS attack announcements made on the web since December, 2010. The final list of announcements that were evaluated for this study are shown in Table 1. It also shows the total number of negative, positive and no impact periods in each case. In total 60 DDoS attack announcements were considered for this study. We further filtered these announcements on the basis of the following criteria:

- In case of multiple announcements made on consecutive days, the earliest announcement was considered.
- All announcements in relation with companies that were not publicly traded at the time attack were removed from the dataset.
- All such announcements that reported DDoS attacks were coupled with integrity and confidentiality attacks were not considered. This was done to analyze the impact of DDoS attack announcements in isolation on the company's stock price.

The above criterion of filtering is consistent with previous studies [8]. Yahoo! finance was used in order to collect stock prices for all the firms. We used S&P 500 index values for calculating the market rate (r_{mt}). Standard and Poor's (S&P) 500 has been used by many of the previous studies as the index of the market. Finally, after filtering the initial dataset we analyze a sample of 45 announcements.

3.2 Analysis

For analysis of the data set we first establish the null hypothesis (H_0) as follows:

H_0**:** *There is no impact of DDoS attack announcements on victim stock prices.*

In order to analyze the collected data we first need to calculate the rate of return of the market index on day t (r_{mt}) and r_{it} the rate of return of the stock i on day t. The rate of return can be calculated as shown in Equation 5, where R_{it} and R_{mt} represent the stock price and market index for day t. The value of the market index shows the average of returns of all the firms included in the market index.

$$\begin{aligned} r_{it} &= \frac{R_{it} - R_{i(t-1)}}{R_{i(t-1)}} \\ r_{mt} &= \frac{R_{mt} - R_{m(t-1)}}{R_{m(t-1)}} \end{aligned} \tag{5}$$

We use three different methods to test our null hypothesis (H_0). After explaining in detail these methods in Sections 3.2.1, 3.2.2 and 3.2.3 we then compare the results in Section 4 and conclude in Section 5.

3.2.1 Method 1

In the first method we consider an additive model to represent the normal behavior of the market. The model can be mathematically represented as shown by Equation 6. This model is used to estimate the returns on a firm's stock. The parameters r_{it} and r_{mt} are calculated as shown in Equation 5.

$$r_{it} = \alpha_i + \beta_i r_{mt} + \varepsilon_{it} \tag{6}$$

The stochastic variable ε_{it} is the error term with $\mathbb{E}[\varepsilon_{it}] = 0$. We use ordinary least squares (OLS) in order to calculate the estimations $\hat{\alpha}_i$ and $\hat{\beta}_i$ for the firm dependent parameters α_i and β_i by considering daily returns over a period of 200 days. The estimation period starts 201 days before the date of attack announcement and ends two days before the announcement.

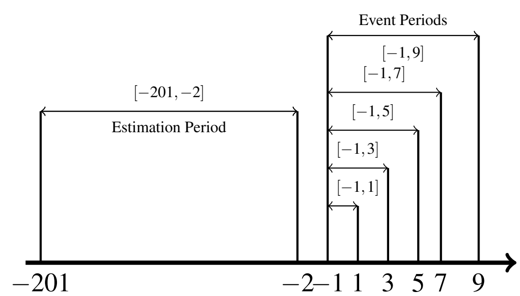


Figure 3: Estimation and Event Periods.

The additive abnormal return (AAR_{it}) is the measurement of the deviation of the actual returns from the ones calculated with the help of additive model (Equation 6). Hence AAR_{it} can be mathematically represented as:

$$AAR_{it} = r_{it} - (\hat{\alpha}_i + \hat{\beta}_i r_{mt}) \tag{7}$$

We measure the impact of DDoS attack announcements on the stock return over the following five *event periods*:

1. One day prior to the announcement to 1 days after it $[t-1, t+1]$.
2. One day prior to the announcement to 3 days after it $[t-1, t+3]$.
3. One day prior to the announcement to 5 days after it $[t-1, t+5]$.
4. One day prior to the announcement to 7 days after it $[t-1, t+7]$.
5. One day prior to the announcement to 9 days after it $[t-1, t+9]$.

We use the same time periods for all methods in our analysis. The *estimation period* and the *event periods* are shown in Figure 3. We take the event periods from one day prior to the announcements in order to compensate for any time lags. In order to calculate the combined effect over a certain number of days, we calculate the additive cumulative abnormal return (*ACAR*) as shown in Equation 8 for the period $[N_1, N_2]$.

$$ACAR_i = \sum_{t=N_1}^{N_2} (AAR_{it}) \tag{8}$$

We compute the mean *ACAR* for 45 events in our sample as follows:

$$ACAR = \frac{1}{K} \sum_{i=1}^{K} ACAR_i \tag{9}$$

Where K is the number of events. We then estimate the standard deviation (σ_{ACAR}) using Equation 10.

$$\sigma_{ACAR} = \sqrt{\frac{\sum_{i=1}^{K} (ACAR_i - ACAR)^2}{K-1}} \tag{10}$$

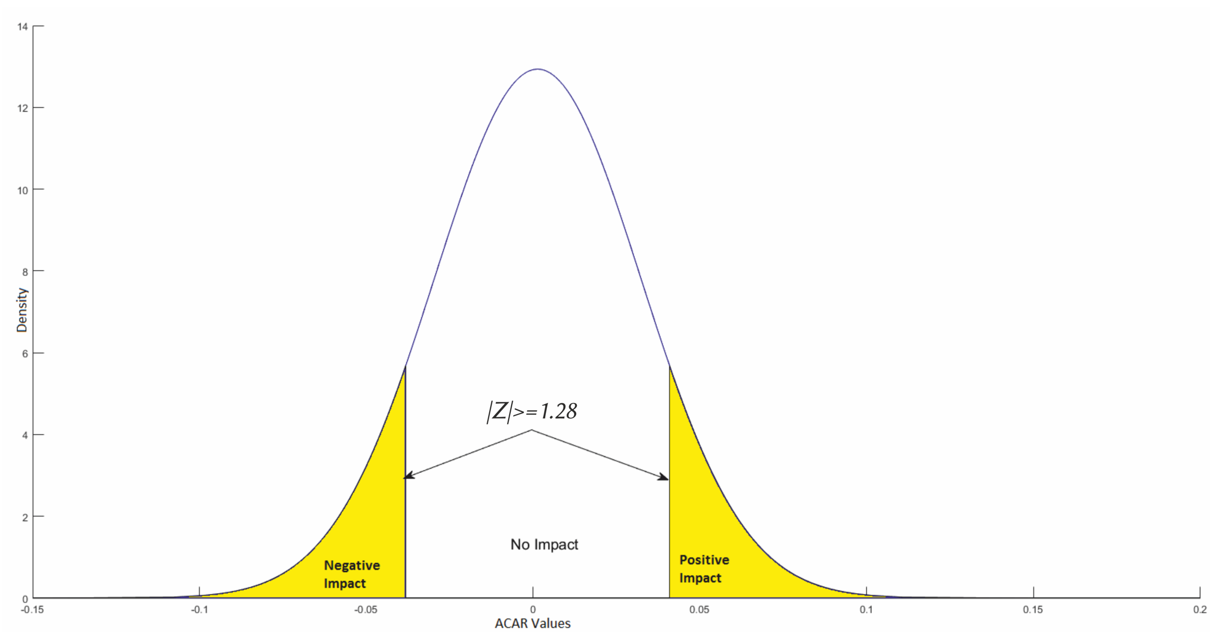
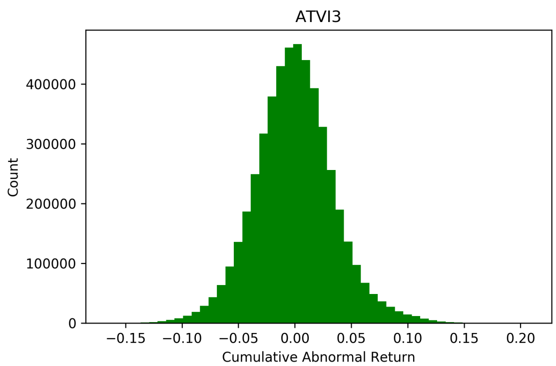


Figure 4: Normal distribution for 5 day *ACAR* values and decision rule for impact analysis.

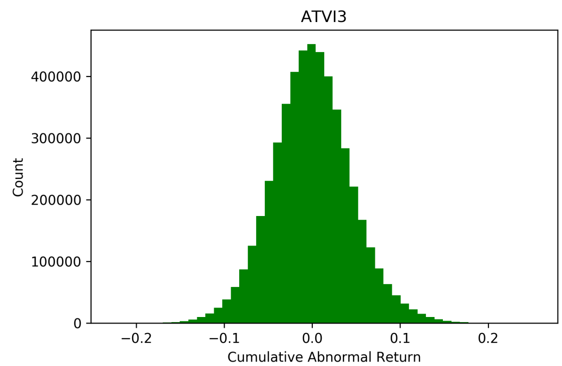
We now assume the $ACAR_i$ values for a given *event period* to be normally distributed and test for significance by making use of the Z-statistic at 10% confidence level. Hence we reject the null hypothesis if the $|Z| >= 1.282$ as shown in Figure 4.

3.2.2 Method 2

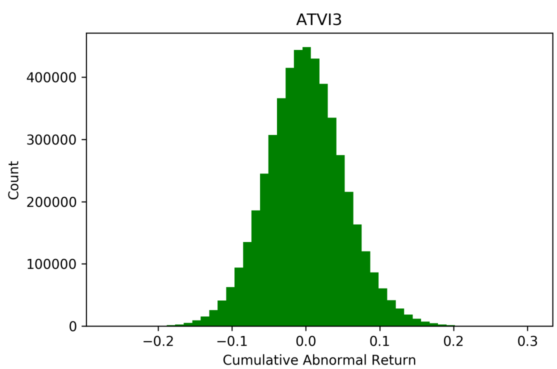
In this method we again make use of the additive estimation model as shown in Equation 6. We avoid the widespread assumption of short-term returns being approximately normally distributed. We also do not impose any alternative distribution to these returns. Instead we use the technique of bootstrapping (e.g. Efron [15]). In this case we generate 5 million n-day returns by randomly drawing n one-day returns from the empirical distribution. The relative frequencies of these 5 million multi-day returns are then used as the distribution for hypothesis testing.



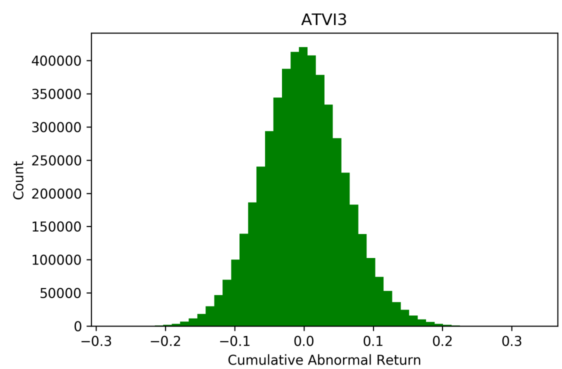
(a) 3-Day $ACAR_{ActivisionBlizzard}$



(b) 5-Day $ACAR_{ActivisionBlizzard}$



(c) 7-Day $ACAR_{ActivisionBlizzard}$



(d) 9-Day $ACAR_{ActivisionBlizzard}$

Figure 5: Empirical distribution of $ACAR$(additive) for Activision Blizzard

In order to calculate the additive abnormal returns we again employ Equation 7. After computing the AAR_{it}s for the estimation period and the event periods as discussed in Section 3.2.1 we draw 3, 5, 7, 9 and 11 one-day abnormal returns from the estimation period AARs. We then calculate the value of $ACAR_i$ for each of these scenarios with the help of Equation 8. Figure 5 shows the empirical distribution of $ACAR$ for Activision Blizzard. Lastly, to asses the effect of DDoS attack announcement on the stock returns we check the position of $ACAR_i$ for a certain event period in the empirical distribution of $ACAR$ for the same number of days of firm i. For example, if we are evaluating the $ACAR$ of Activision Blizzard for event period $[t-1, t+1]$ then we check the position of this $ACAR$ in the 3-day empirical distribution for Activision Blizzard. In this study we consider the 10 percentile scenarios in the left tail to be representative of negative impact and 10 percentile scenarios to the right for positive impact. Hence, if $ACAR_i$ is negative and lies in the bottom 10 percentile of the 5 million scenarios then the impact on the stock returns is considered to be negative.

3.2.3 Method 3

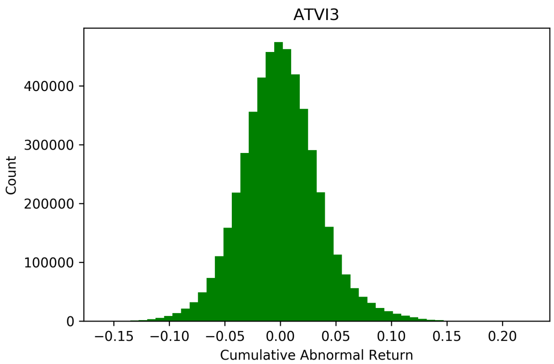
In this final method we use a multiplicative model for the estimation of stock returns. The multiplicative estimation model is shown in Equation 11.

$$(1 + r_{it}) = \alpha_i (1 + r_{mt})^{\beta_i} \tag{11}$$

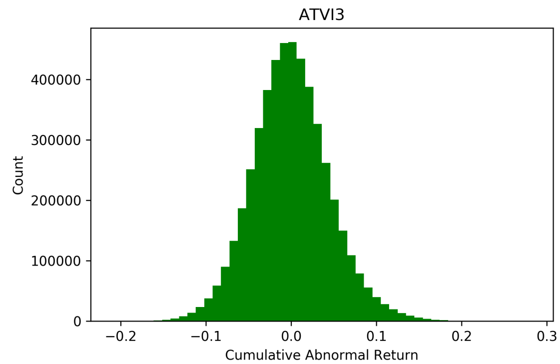
Also, this time we also deviate from the wide spread practice of adding the corresponding single-day returns to compute the cumulative returns. Instead we calculate the exact cumulative returns[1].

We linearize Equation 11 by taking logarithms as shown in Equation 12. The stochastic variable ε_{it} represents the error term with $\mathbb{E}\left[\varepsilon_{it}\right] = 0$.

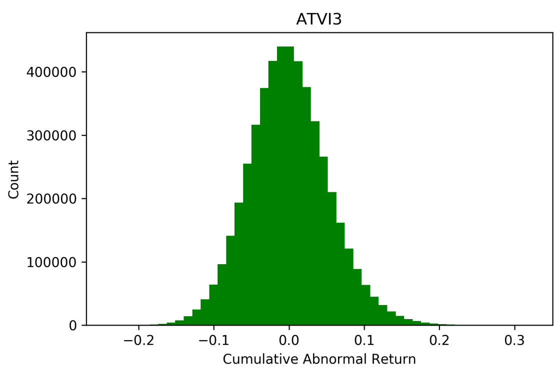
$$\ln(1+r_{it}) = \widehat{\ln(\alpha_i)} + \hat{\beta}_i \ln(1+r_{mt}) + \varepsilon_{it} \tag{12}$$



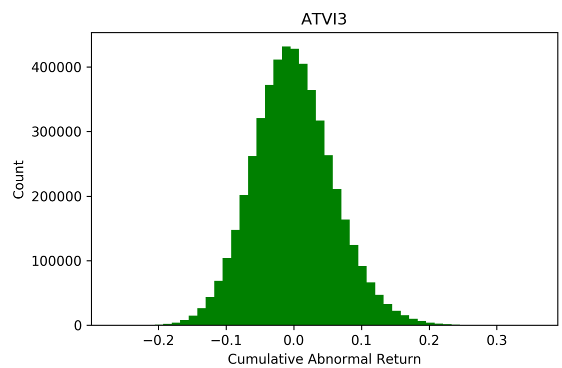
(a) 3-Day $CAR_{ActivisionBlizzard}$



(b) 5-Day $CAR_{ActivisionBlizzard}$



(c) 7-Day $CAR_{ActivisionBlizzard}$



(d) 9-Day $CAR_{ActivisionBlizzard}$

Figure 6: Empirical distribution of CAR(multiplicative) for Activision Blizzard

After estimating the stock returns we use Equation 13 for computing the abnormal returns. As $\widehat{\ln(\alpha_i)}$ is a biased estimator for α_i ($\mathbb{E}\left[\hat{\alpha}_i\right] \neq \mathbb{E}\left[e^{\widehat{\ln \alpha_i}}\right]$), we use Equation 14 for estimating $\hat{\alpha}_i$.

$$AR_{it} = \frac{(1+r_{it})}{\hat{\alpha}_i(1+r_{mt})^{\hat{\beta}_i}} - 1 \tag{13}$$

$$\hat{\alpha}_i = \frac{\sum_{t=1}^{T}(1+r_{it})}{\sum_{t=1}^{T}(1+r_{mt})^{\hat{\beta}_i}}, \tag{14}$$

After computing the AR_{it}s for the estimation period and the event periods as discussed in Section 3.2.1 we draw 3, 5, 7, 9 and 11 one-day abnormal returns from the estimation period ARs. As discussed

[1] An increase of 10%, followed by a 10% decrease implies a total decrease of 1% according to the multiplicative formula $(1.1)(0.9) = 0.99$. The additive approximation yields a change of 0%, which is an overestimation of 1%.

earlier we then calculate the value of CAR_i for each of these scenarios with the help of Equation 15.

$$CAR = \prod_{t=N_1}^{N_2} (1 + AR_{it}) - 1 \tag{15}$$

Figure 6 shows the empirical distribution of *CAR* for Activision Blizzard. Lastly, to asses the effect of DDoS attack announcements on the stock returns we check the position of CAR_i for a certain event period in the empirical distribution of *CAR* for the same number of days of firm *i*. For example, if we are evaluating the *CAR* of Activision Blizzard for event period $[t-1, t+1]$ then we check the position of this *CAR* in the 3-day empirical distribution for Activision Blizzard. In this study we consider the 10 percentile scenarios in the left tail to be representative of negative impact and 10 percentile scenarios to the right for positive impact. Hence, if CAR_i is negative and lies in the bottom 10 percentile of the 5 million scenarios then the impact on the stock returns is considered to be negative.

In the next section we discuss the results of our analysis and compare the results.

4 Results and Discussion

We now compare the results of our analysis. Table 1 summarizes the outcomes of using the three different methods. The table shows the number of positive and negative *event periods* in each case. A negative event periods imply that the DDoS attack announcement did impact investor decisions. The positive event periods on the stock price actually show that the stock was well performing and the DDoS attack announcement did not have any impact on the stock price. Later in Appendix A we present the impact on each firm analyzed in detail.

First we compare the differences in the results due to the choice of Method 2 and Method 3. Both methods do not take the assumption of normal distribution for assessing cumulative abnormal returns. However, Method 2 uses an additive model for estimation and Method 3 uses a multiplicative model for the return rate estimation. We find no differences between the results of the two models in the periods analyzed. Hence, we can conclude that the additive model does provide a satisfactory estimation for the computation of cumulative abnormal returns. The choice of estimation model has no impact on the outcomes, if an empirical distribution of cumulative abnormal returns is used to test the hypothesis.

Then we look for differences in the results of Method 1 and Method 3. The differences between the models are as follows:

- Method 1 and Method 2 both use an additive estimation model for calculating cumulative abnormal.
- Method 1 assumes the cumulative abnormal returns to be normally distributed for hypothesis testing, where as Method 2 employs the empirical distribution of cumulative abnormal returns to test the hypothesis.
- Finally, Method 3 uses a multiplicative estimation model for calculating cumulative abnormal returns and uses the empirical distribution of cumulative abnormal returns to test the hypothesis.

Table 3 summarizes the differences between the two methods. We believe that Method 3 is more accurate, or rather less inaccurate, than Method 1 due to the reduced number of assumptions and approximations in the model. Hence, look at the number of times Method 1 overestimates or underestimates the significance of the results, i.e. gives a significant positive or negative impact when there is no impact or vice-versa. We observe that Method 1 overestimates the significance of the abnormal returns 5.77% (total 225 periods are considered in this study) of the times and underestimates it 7.55% of the times.

		Method 1			Method 2			Method 3		
Company Name	Date	+ve periods	-ve periods	No impact	+ve periods	-ve periods	No impact	+ve periods	-ve periods	No impact
Master Card	2010-12-07	2	1	2	2	0	3	2	0	3
Visa	2010-12-07	2	2	1	2	1	2	2	1	2
Bank of America	2010-12-27	0	3	2	0	3	2	0	3	2
Vodafone	2011-10-04	0	0	5	0	0	5	0	0	5
Vivendi	2012-01-18	0	0	5	0	0	5	0	0	5
Bursa Malaysia	2012-02-13	0	0	5	0	0	5	0	0	5
Apple	2012-05-25	0	1	4	0	0	5	0	0	5
AT&T	2012-08-15	0	0	5	1	0	4	1	0	4
Wells Fargo	2012-12-19	0	0	5	0	0	5	0	0	5
JP Morgan Chase	2013-03-12	0	0	5	3	0	2	3	0	2
TD Canada Trust	2013-03-20	0	0	5	0	1	4	0	1	4
American Express	2013-03-27	0	0	5	1	0	4	1	0	4
ING	2013-04-08	0	3	2	0	2	3	0	2	3
Linkedin	2013-06-20	0	1	4	0	0	5	0	0	5
Microsoft	2013-11-26	0	0	5	0	0	5	0	0	5
RBS	2013-12-03	0	0	5	0	0	5	0	0	5
Electronic Arts	2014-01-02	0	0	5	0	0	5	0	0	5
JP Morgan Chase	2014-01-29	0	0	5	0	0	5	0	0	5
Bank of America	2014-01-29	0	0	5	0	0	5	0	0	5
Facebook	2014-02-20	0	0	5	0	0	5	0	0	5
Verizon Communications	2014-03-21	0	0	5	0	0	5	0	0	5
Activision Blizzard	2014-03-28	1	0	4	2	0	3	2	0	3
Danske Bank	2014-07-09	0	0	5	0	0	5	0	0	5
Storebrand	2014-07-09	0	0	5	0	0	5	0	0	5
Gjensidige Forsikr	2014-07-09	0	3	2	0	4	1	0	4	1
Sony	2014-08-22	0	0	5	0	0	5	0	0	5
Amazon	2014-08-26	0	0	5	0	0	5	0	0	5
Activision Blizzard	2014-11-13	2	1	2	1	2	2	1	2	2
Sony	2014-11-25	0	0	5	0	0	5	0	0	5
Rackspace	2014-12-19	0	0	5	0	0	5	0	0	5
Microsoft	2014-12-23	0	0	5	3	0	2	3	0	2
Sony	2014-12-23	0	0	5	0	0	5	0	0	5
Alibaba	2014-12-24	1	0	4	0	0	5	0	0	5
Nordea Bank	2015-01-09	0	3	2	0	3	2	0	3	2
Facebook	2015-01-26	0	0	5	0	0	5	0	0	5
Amazon	2015-03-13	0	0	5	0	0	5	0	0	5
Electronic Arts	2015-03-17	0	4	1	0	1	4	0	1	4
Ziggo (Liberty Global)	2015-08-17	2	0	3	4	0	1	4	0	1
Overstock.com	2015-09-02	0	0	5	0	0	5	0	0	5
Nissan	2016-01-12	1	0	4	0	0	5	0	0	5
HSBC	2016-01-28	3	0	2	3	0	2	3	0	2
Activision Blizzard	2016-08-02	0	1	4	0	0	5	0	0	5
Electronic Arts	2016-08-31	0	1	4	0	0	5	0	0	5
StarHub	2016-10-26	0	0	5	2	0	3	2	0	3
Deutsche Telekom	2016-11-28	0	1	4	0	2	3	0	2	3

Table 1: List of victim companies and summary of results

Method 2 \ Method 3	+ve	No	-ve
+ve	24	0	0
No	0	182	0
-ve	0	0	19

Table 2: Cross-table showing the number of differences between Method 2 and Method 3.

We find these differences to be consistent between Method 1 and Method 2 as well. This suggests that the assumption of normally distributed abnormal returns accounts for these inconsistencies between the results of Method 1 and Method 3 (or Method 2).

Method 1 \ Method 3	+ve	No	-ve
+ve	11	3	0
No	13	169	4
-ve	0	10	15

Table 3: Cross-table showing the number of differences between Method 1 and Method 3.

5 Conclusion

As an outcome of our study we draw two main conclusions. First, by comparing the various methods of conducting event studies we bring out the risk of overestimating or underestimating the impact of DDoS attack announcements on victims' stock prices. The choice of additive or multiplicative model does not affect the results but the assumption of normally distributed cumulative returns can lead to an incorrect estimation of the impact. Hence, in this study we propose the use of an empirical distribution in order to check the significance of cumulative abnormal returns. Secondly, we also re-emphasize on the results of our previous study [8], and show that all three methods result in a significantly negative event periods on stock price when service to the customers was hampered due to the attack. We reported that the attacks on International Nederlanse Group (ING) and Nordea bank [16, 17] resulted in significant negative returns where as Visa and Mastercard [18] resulted in no damage. Similarly, in case of the attack on Deutsche Telekom that drove nearly 1 million of its customers offline [19], we observe a negative impact on the stock price in the 9-day and 11-day period.

References

[1] R. Anderson, C. Barton, R. Böhme, , R. Clayton, M. J. G. van Eeten, M. Levi, T. Moore, and S. Savage, *Measuring the Cost of Cybercrime*. Springer, Berlin, Heidelberg, 2013, pp. 265–300.

[2] "Dyn statement on 10/21/2016 ddos attack," http://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/ [Online; Accessed on November 17, 2017], 2016.

[3] "Oracle just bought the company that brought down the internet." https://www.wired.com/2016/11/oracle-just-bought-dyn-company-brought-internet/ [Online; Accessed on November 17, 2017], 2016.

[4] A. C. Mackinlay, "Event Studies in Economics and Finance." *American Economic Association*, vol. 35, pp. 13–39, March 1997.

[5] P. C. Tetlock, "Giving content to investor sentiment: The role of media in the stock market," *The Journal of Finance*, vol. 62, no. 3, pp. 1139–1168, May 2007.

[6] D. Florêncio and C. Herley, "Sex, lies and cyber-crime surveys," in *Economics of Information Security and Privacy III*, B. Schneier, Ed. Springer, New York, NY, 2013, pp. 35–53.

[7] B. L. Dos Santos, K. Peffers, and D. C. Mauer, "The impact of information technology investment announcements on the market value of the firm," *Information Systems Research*, vol. 4, no. 1, pp. 1–23, March 1993.

[8] Abhishta, R. Joosten, and L. J. M. Nieuwenhuis, "Analysing the Impact of a DDoS Attack Announcement on Victim Stock Prices," in *Proc. of the 25th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP'17), St. Petersburg, Russia*. IEEE, March 2017, pp. 354–362.

[9] A. Hovav and J. D'Arcy, "Impact of Denial-of-Service attack announcements on the market value of firms," *Risk Management And Insurance Review*, vol. 6, no. 2, pp. 97–121, September 2003.

[10] K. Campbell, L. A. Gordon, M. P. Loeb, and L. Zhou, "The Economic Cost of Publicly Announced Information Security Breaches : Empirical Evidence from the Stock Market," *Journal of Computer Security*, vol. 11, no. 3, pp. 431–448, March 2003.

[11] H. Cavusoglu, B. Mishra, and S. Raghunathan, "The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers," *International Journal of Electronic Commerce*, vol. 9, no. 1, pp. 70–104, October 2004.

[12] K. Kannan, J. Rees, and S. Sridhar, "Market Reactions to Information Security Breach Announcements: An Empirical Analysis," *International Journal of Electronic Commerce*, vol. 12, no. 1, pp. 69–91, December 2007.

[13] L. A. Gordon, M. P. Loeb, and L. Zhou, "The impact of information security breaches : Has there been a downward shift in costs?" *Journal of Computer Security*, vol. 19, no. 1, pp. 33–56, January 2011.

[14] E. Fama and K. French, "Common risk factors in the returns of stocks and bonds," *Journal of Financial Economics*, vol. 33, no. 1, pp. 3–56, February 1993.

[15] B. Efron, "Bootstrap methods: another look at the jackknife," in *Breakthroughs in Statistics*, ser. Springer Series in Statistics, S. Kotz and N. L. Johnson, Eds. Springer, New York, NY, 1992, pp. 569–593.

[16] "Ing ondanks maatregelen getroffen door nieuwe ddos-aanval," http://www.nrc.nl/nieuws/2013/04/10/ing-nieuwe-cyberaanval-sneller-afgeslagen-door-maatregelen [Online; Accessed on November 17, 2017], 2013.

[17] "Norway banks hit in largest-ever ddos attack, anonymous takes credit," http://ddosattacks.net/norway-banks-hit-in-largest-ever-ddos-attack-anonymous-takes-credit/ [Online; Accessed on November 17, 2017], 2014.

[18] "Wikileaks supporters disrupt visa and mastercard sites in 'operation payback'," https://www.theguardian.com/world/2010/dec/08/wikileaks-visa-mastercard-operation-payback [Online; Accessed on November 17, 2017], 2010.

[19] "Failed mirai botnet attack downed 900000 germans' internet access." https://www.siliconrepublic.com/enterprise/mirai-botnet-deutsche-telekom [Online; Accessed on November 17, 2017], 2016.

Author Biography

Abhishta(1991) is a full-time Ph.D. candidate at the department of Industrial Engineering and Business Information Systems at the University of Twente. He did his bachelor in Industrial Engineering and Masters in Business Administration. His research involves analyzing the economic and social impact of distributed denial of service (DDoS) attacks. His research is funded by the Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO) under award number: 628.001.018.

Reinoud Joosten is an assistant professor at the Industrial Engineering and Business Information Systems department of the University of Twente, The Netherlands. He obtained his Ph.D. from Maastricht University in 1996. He spent several years as a Post Doc at Maastricht University and the Max Planck Institute for Economics in Jena, Germany. He has been at the University of Twente since 2001. His research interests include game theory, operations research, economics, finance, and more specifically: strategic and economic aspects of DDoS attacks. He is an advisory editor of the Journal of Evolutionary Economics.

Lambert J. M. Nieumenhuis (1955) is a full professor in Quality of Service of Telematics Systems at the department of Industrial Engineering and Business Information Systems at the University of Twente. He is professor in Business Service Innovation at the Fontys International Business School of the Fontys University of Applied Sciences. He is owner and managing partner of the consultancy firm Knowledge for Business Innovation. Previously, he worked more than 20 years for KPN Research, the R&D facility of KPN, the telephony and Internet market leader in The Netherlands. Bart Nieuwenhuis holds a Bsc and MSc in Electrical Engineering (cum laude) and a PhD in Computer Science.

A Impact on victim stock prices

Firm	Event Period	Method 1	Method 2	Method 3
Bursa Malaysia	3-day	No	No	No
	5-day	No	No	No
	7-day	No	No	No
	9-day	No	No	No
	11-day	No	No	No
Apple	3-day	-ve	No	No
	5-day	No	No	No
	7-day	No	No	No
	9-day	No	No	No
	11-day	No	No	No
Amazon	3-day	No	No	No
	5-day	No	No	No
	7-day	No	No	No
	9-day	No	No	No
	11-day	No	No	No
Amazon	3-day	No	No	No
	5-day	No	No	No
	7-day	No	No	No
	9-day	No	No	No
	11-day	No	No	No
Activision Blizzard	3-day	+ve	No	No
	5-day	+ve	+ve	+ve
	7-day	No	No	No
	9-day	-ve	-ve	-ve
	11-day	No	-ve	-ve
Activision Blizzard	3-day	No	No	No
	5-day	No	No	No
	7-day	+ve	+ve	+ve
	9-day	No	No	No

Firm	Event Period	Method 1	Method 2	Method 3
	11-day	No	+ve	+ve
Activision Blizzard	3-day	-ve	No	No
	5-day	No	No	No
	7-day	No	No	No
	9-day	No	No	No
	11-day	No	No	No
American Express	3-day	No	No	No
	5-day	No	No	No
	7-day	No	No	No
	9-day	No	+ve	+ve
	11-day	No	No	No
Alibaba	3-day	No	No	No
	5-day	No	No	No
	7-day	+ve	No	No
	9-day	No	No	No
	11-day	No	No	No
Bank of America	3-day	No	No	No
	5-day	No	No	No
	7-day	-ve	-ve	-ve
	9-day	-ve	-ve	-ve
	11-day	-ve	-ve	-ve
Bank of America	3-day	No	No	No
	5-day	No	No	No
	7-day	No	No	No
	9-day	No	No	No
	11-day	No	No	No
StarHub	3-day	No	No	No
	5-day	No	No	No
	7-day	No	No	No
	9-day	No	+ve	+ve
	11-day	No	+ve	+ve
Danske Bank	3-day	No	No	No
	5-day	No	No	No
	7-day	No	No	No
	9-day	No	No	No
	11-day	No	No	No
Deutsche Telekom	3-day	No	No	No
	5-day	No	No	No
	7-day	No	No	No
	9-day	-ve	-ve	-ve
	11-day	No	-ve	-ve
	3-day	-ve	No	No

Firm	Event Period	Method 1	Method 2	Method 3
Electronic Arts	5-day	-ve	-ve	-ve
	7-day	No	No	No
	9-day	-ve	No	No
	11-day	-ve	No	No
Electronic Arts	3-day	No	No	No
	5-day	No	No	No
	7-day	No	No	No
	9-day	No	No	No
	11-day	No	No	No
Electronic Arts	3-day	-ve	No	No
	5-day	No	No	No
	7-day	No	No	No
	9-day	No	No	No
	11-day	No	No	No
Facebook	3-day	No	No	No
	5-day	No	No	No
	7-day	No	No	No
	9-day	No	No	No
	11-day	No	No	No
Facebook	3-day	No	No	No
	5-day	No	No	No
	7-day	No	No	No
	9-day	No	No	No
	11-day	No	No	No
Gjensidige Forsikr	3-day	No	No	No
	5-day	-ve	-ve	-ve
	7-day	-ve	-ve	-ve
	9-day	-ve	-ve	-ve
	11-day	No	-ve	-ve
Activision Blizzard	3-day	No	No	No
	5-day	+ve	+ve	+ve
	7-day	No	No	No
	9-day	+ve	+ve	+ve
	11-day	+ve	+ve	+ve
ING	3-day	-ve	-ve	-ve
	5-day	-ve	No	No
	7-day	-ve	-ve	-ve
	9-day	No	No	No
	11-day	No	No	No
JP Morgan Chase	3-day	No	No	No
	5-day	No	No	No
	7-day	No	No	No
	9-day	No	No	No

Firm	Event Period	Method 1	Method 2	Method 3
	11-day	No	No	No
JP Morgan Chase	3-day	No	No	No
	5-day	No	No	No
	7-day	No	+ve	+ve
	9-day	No	+ve	+ve
	11-day	No	+ve	+ve
Ziggo (Liberty Global)	3-day	No	No	No
	5-day	+ve	+ve	+ve
	7-day	+ve	+ve	+ve
	9-day	No	+ve	+ve
	11-day	No	+ve	+ve
Linkedin	3-day	No	No	No
	5-day	No	No	No
	7-day	No	No	No
	9-day	No	No	No
	11-day	-ve	No	No
Master Card	3-day	No	No	No
	5-day	-ve	No	No
	7-day	No	No	No
	9-day	+ve	+ve	+ve
	11-day	+ve	+ve	+ve
Microsoft	3-day	No	No	No
	5-day	No	No	No
	7-day	No	No	No
	9-day	No	No	No
	11-day	No	No	No
Microsoft	3-day	No	No	No
	5-day	No	+ve	+ve
	7-day	No	+ve	+ve
	9-day	No	+ve	+ve
	11-day	No	No	No
Nordea Bank	3-day	No	No	No
	5-day	No	No	No
	7-day	-ve	-ve	-ve
	9-day	-ve	-ve	-ve
	11-day	-ve	-ve	-ve
Nissan	3-day	No	No	No
	5-day	No	No	No
	7-day	+ve	No	No
	9-day	No	No	No
	11-day	No	No	No
	3-day	No	No	No

Firm	Event Period	Method 1	Method 2	Method 3
Overstock.com	5-day	No	No	No
	7-day	No	No	No
	9-day	No	No	No
	11-day	No	No	No
Rackspace	3-day	No	No	No
	5-day	No	No	No
	7-day	No	No	No
	9-day	No	No	No
	11-day	No	No	No
RBS	3-day	No	No	No
	5-day	No	No	No
	7-day	No	No	No
	9-day	No	No	No
	11-day	No	No	No
Sony	3-day	No	No	No
	5-day	No	No	No
	7-day	No	No	No
	9-day	No	No	No
	11-day	No	No	No
Sony	3-day	No	No	No
	5-day	No	No	No
	7-day	No	No	No
	9-day	No	No	No
	11-day	No	No	No
Sony	3-day	No	No	No
	5-day	No	No	No
	7-day	No	No	No
	9-day	No	No	No
	11-day	No	No	No
Storebrand	3-day	No	No	No
	5-day	No	No	No
	7-day	No	No	No
	9-day	No	No	No
	11-day	No	No	No
AT&T	3-day	No	No	No
	5-day	No	+ve	+ve
	7-day	No	No	No
	9-day	No	No	No
	11-day	No	No	No
TD Canada Trust	3-day	No	No	No
	5-day	No	No	No
	7-day	No	No	No
	9-day	No	-ve	-ve

Firm	Event Period	Method 1	Method 2	Method 3
	11-day	No	No	No
Visa	3-day	-ve	No	No
	5-day	-ve	-ve	-ve
	7-day	No	No	No
	9-day	+ve	+ve	+ve
	11-day	+ve	+ve	+ve
Vivendi	3-day	No	No	No
	5-day	No	No	No
	7-day	No	No	No
	9-day	No	No	No
	11-day	No	No	No
Vodafone	3-day	No	No	No
	5-day	No	No	No
	7-day	No	No	No
	9-day	No	No	No
	11-day	No	No	No
Verizon Communications	3-day	No	No	No
	5-day	No	No	No
	7-day	No	No	No
	9-day	No	No	No
	11-day	No	No	No
Wells Fargo	3-day	No	No	No
	5-day	No	No	No
	7-day	No	No	No
	9-day	No	No	No
	11-day	No	No	No

*The multiple events related to the same firm are sorted date wise.