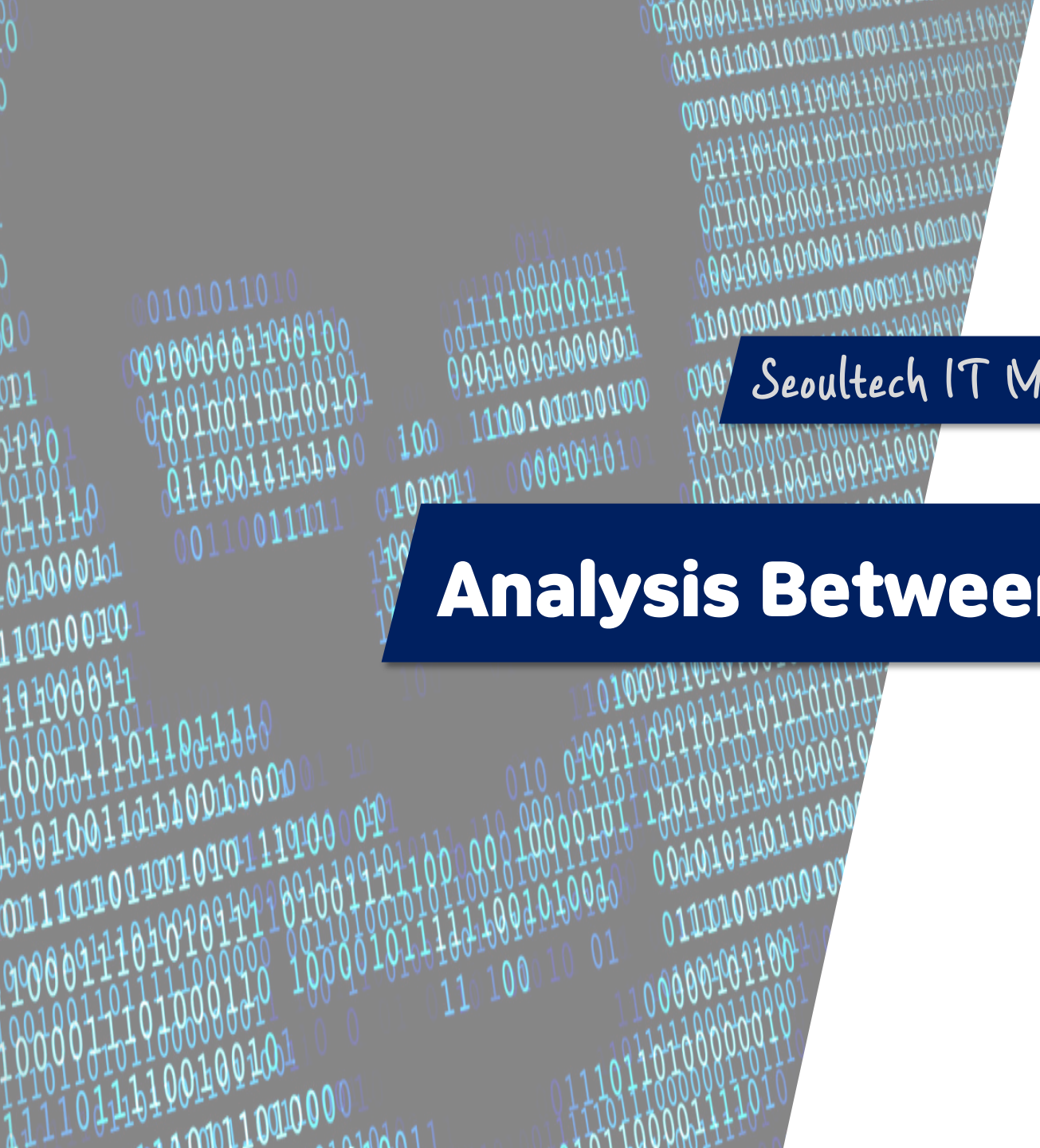


Seoultech IT Management 2019 Capstone Design Final Presentation

Analysis Between Cyberattacks and Tweets

14146320 **Junha** Lee

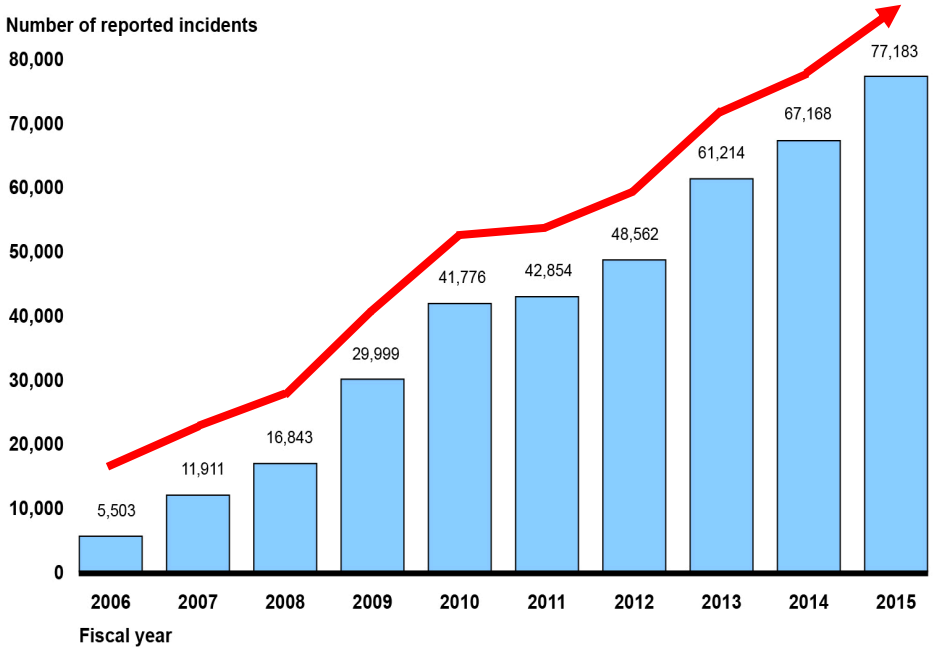
15146326 **Boyoung** Han

SEOULTECH
SEOUL NATIONAL UNIVERSITY OF SCIENCE & TECHNOLOGY

Northumbria University
NEWCASTLE

1. Background & Goal

Figure 1: Cyberattacks Reported by Federal Agencies

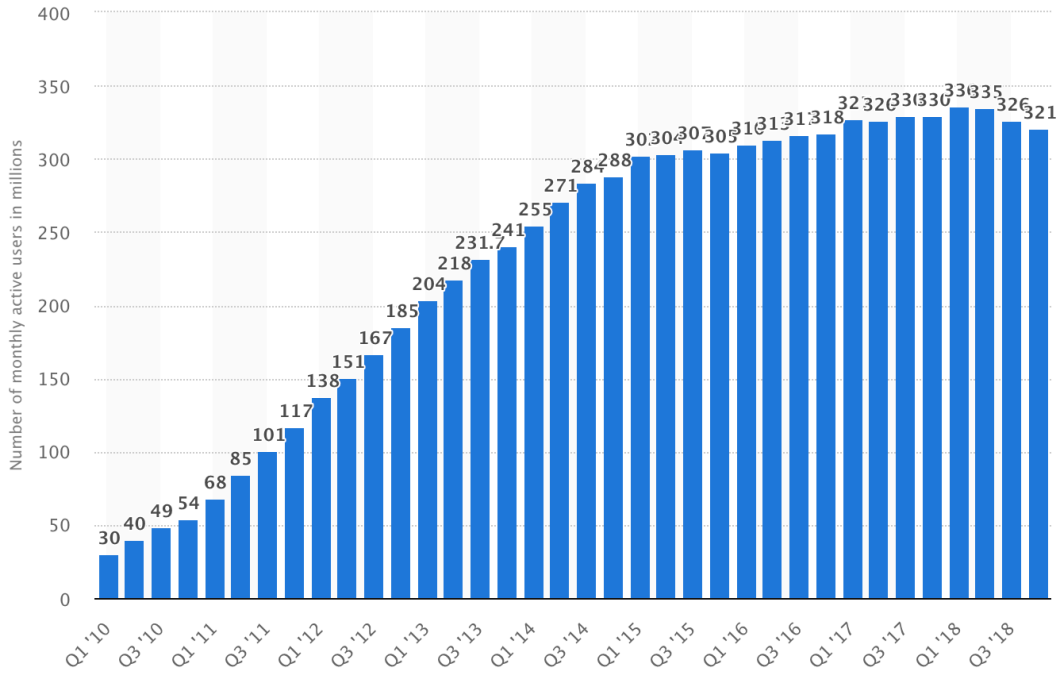


Source: GAO analysis of United States Computer Emergency Readiness Team and Office of Management and Budget data for fiscal years 2006-2015. | GAO-16-885T

An increase in cyberattacks each year

→ Threats about cyberattacks are increasing

Figure 2 : Number of monthly active Twitter user



The number of twitters sent every day

→ Lots of information in Twitter

➔ **Find Relations** between **Cyber Attack** and **Hackers' Tweets**

2. Related Work & Differentiation

- Analyzing the Perceived Severity of Cybersecurity Threats Reported on Social Media
  - Analysis of text referring to the severity of cyberattacks online based on specific keywords
- Discovering Signals from Web Sources to Predict Cyber Attacks
  - Predict attack by analyzing cyber threats by analyzing articles posted on various websites through ML
- Detecting Denial-of-Service Attacks from Social Media Text : Applying NLP to Computer Security
  - Analysis of SNS users' responses to cyberattack(DDoS) using NLP models

➔ Common point : Predict cyberattack using SNS(Twitter) data

- **Different Point**
  - Focus on Graph database(user network)
  - Time-series(frequency of tweets)

3. Project Process

Data Collection

- Tweepy
- Scrapy
- NEWS Data

Network Graph Analysis

- User Relation
- Group Clustering
- Make Criteria

Frequency Graph Analysis

- Tweet data
- Key-word Filter
- Make Criteria

Relation Analysis

- Network Group
- Frequency

→ Relation Analysis

3-1. Data Collection

Data for	Way to Collect	Collected Data	Properties
All	-	• User **Screen Name** • **Keyword** Related to Cyberattack	• Provided by **Recorded Future** • Order by Priority
Network Graph	Tweepy	• **Following / Follower** • User ID • User Screen Name	• Twitter Developer API • Need Authorized Key • **Request Limitation**

Frequency Graph	Scrapy	• Users' All **Historical Tweets**
		  • User
		  • Date
		  • Text
			• No Limitation
			• One File for One Tweets
			→ **Need to Merge** All json from One user

	Google NEWS	• **Date** of Attack • **Date** of NEWS • Attack Subject • **Importance**	• Real Attack • Search Keyword : **Hit by Cyberattack** • Between 2013 - 2018

3-2. Network Graph Analysis

- Random
  - Choose users randomly in the Recorded Future's List
- Recorded Future (RF)
  - Order provided by Recorded Future's Criteria
- Betweenness Centrality (BC)
  - Detect the amount of influence a node has over the flow of information in a graph
  - Use to find nodes that serve as a bridge from one part of a graph to another
- Closeness Centrality (CC)
  - Detect nodes that are able to spread information very efficiently through a graph
  - Measure its average farness to all other nodes

➔ 4 Criteria for the Users

Table 1 : User number of each Criterion

Criteria	Num of User
Random - (RF U BC U CC)	86
RF - (Random U BC U CC)	15
BC - (Random U RF U CC)	54
CC - (Random U RF U BC)	19
BC ∩ CC	80

Table 2 : Result of Clustering

Criteria	Cluster 1	Cluster 2	Density
Random	65	1 …	65%
Recorded Future	95	1 …	95%
Betweenness	100	-	100%
Closeness	100	-	100%

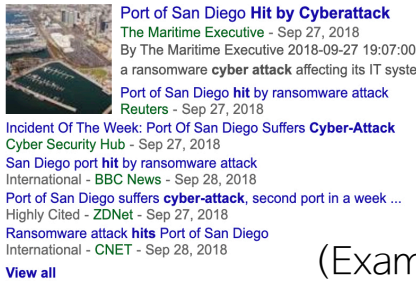
* For each criteria, We choose top 100 people to Analyze *

3-3. Frequency Graph Analysis

- Key-words Filtering
  - Filtered all tweets using key-words related to Cyberattack

```
{"keyword" : "take over Web server"}, {"keyword" : "APT 1"}, {"keyword" : "bypass toll"}
```

- Criteria for News(Attack)
  - All Attack
  - Important Attack
    - Consider the importance of the Cyberattack
  - Adjacent Attack
    - Cyberattack that 'Attack date and News date is adjacent'



(Example of important attack) Importance : 6

	2013	2014	2015	2015	2017	2018	Total
All Attack	12	10	9	8	8	11	58
Important Attack	5	4	4	2	4	4	23
Adjacent Attack	7	7	7	3	3	3	30

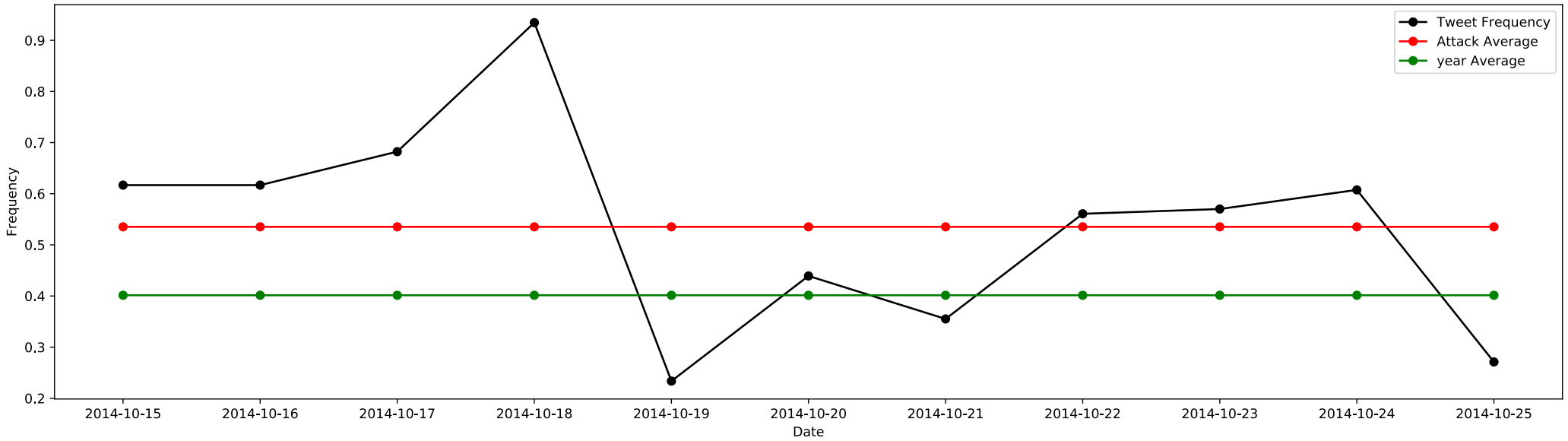
3-4. Analysis

- Criteria for Period
  - Criteria 1 : 15 Days (Before 7 days + Attack Day + After 7 days)
  - Criteria 2 : 11 Days (Before 5 days + Attack Day + After 5 days)
  - Criteria 3 : 7 Days (Before 3 days + Attack Day + After 3 days)

(Consider all criteria)

If an Attack Average is higher than Year Average, that attack is assumed to be related to the tweet activity of users involved in the Cyberattack.

(Attack Avg means the average of given period)



4. Conclusion

R : Random / R_F : Random Filtered / RF : Recorded Future / RF_F : Recorded Future Filtered / BC : Betweenness & Closeness / BC_F : Betweenness & Closeness Filtered

		R	R_F	RF	RF_F	BC	BC_F
Criteria 1 15 Days (Before 7 + Attack + After 7)	All Attack	38.89%	40.68%	42.37%	33.90%	44.07%	49.15%
	Important Attack	34.78%	47.83%	30.43%	34.78%	47.83%	43.48%
	Adjacent Attack	43.33%	50.00%	50.00%	43.33%	40.00%	53.33%
	Avg	39.03%	46.17%	40.93%	37.34%	43.97%	48.65%

		R	R_F	RF	RF_F	BC	BC_F
Criteria 2 11 Days (Before 5 + Attack + After 5)	All Attack	30.51%	38.98%	40.68%	33.90%	42.37%	45.76%
	Important Attack	26.90%	43.48%	30.43%	34.78%	43.48%	39.13%
	Adjacent Attack	36.67%	46.67%	40.00%	40.00%	43.33%	56.67%
	Avg	31.36%	43.04%	37.04%	36.23%	43.06%	47.19%

		R	R_F	RF	RF_F	BC	BC_F
Criteria 3 7 Days (Before 3 + Attack + After 3)	All Attack	37.29%	42.37%	44.07%	32.20%	40.68%	49.15%
	Important Attack	39.13%	52.17%	34.78%	30.43%	47.83%	47.83%
	Adjacent Attack	43.33%	50.00%	50.00%	40.00%	36.67%	60.00%
	Avg	39.92%	48.18%	42.95%	34.21%	42.25%	52.33%

4. Conclusion

	BC_F
Criteria 1 15 Days (Before 7 + Attack + After 7)	49.15%
	43.48%
	53.33%
	48.65%
Criteria 2 11 Days (Before 5 + Attack + After 5)	BC_F
	45.76%
	39.13%
	56.67%
	47.19%
Criteria 1 7 Days (Before 3 + Attack + After 3)	BC_F
	49.15%
	47.83%
	60.00%
	52.33%

1. Sort the Users involved in overall Cyberattacks by **Betweenness Centrality**
2. Filter the Tweets based on **Keywords** related to Cyberattacks

➔ More relevant to Cyberattacks

5. Future Work

1. Subdivide the time series consider the time differences
2. Analyze Tweet text which was written **BEFORE** the attack by using NLP
3. Find deep relationship between users' Tweets and actual cyberattack

➔Possible to **detect** the potential Cyberattack

1. Subdivide the time series consider the time differences
2. Analyze Tweet text which was written **AFTER** the attack by using NLP
3. Find deep relationship between users' Tweets and actual cyberattack

➔Possible to **notify** the Cyberattack as soon as possible