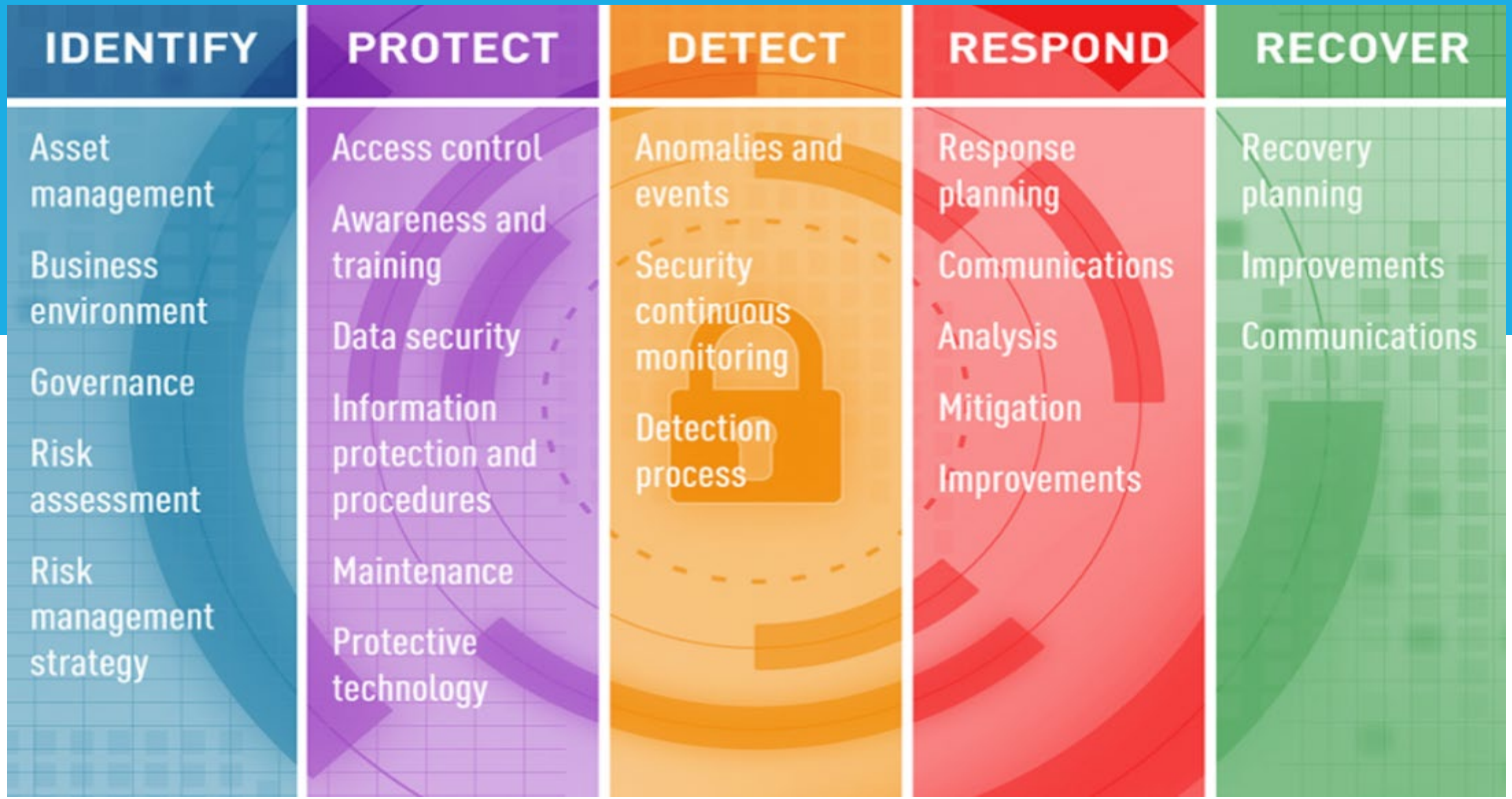
BY KEVIN SPAKES

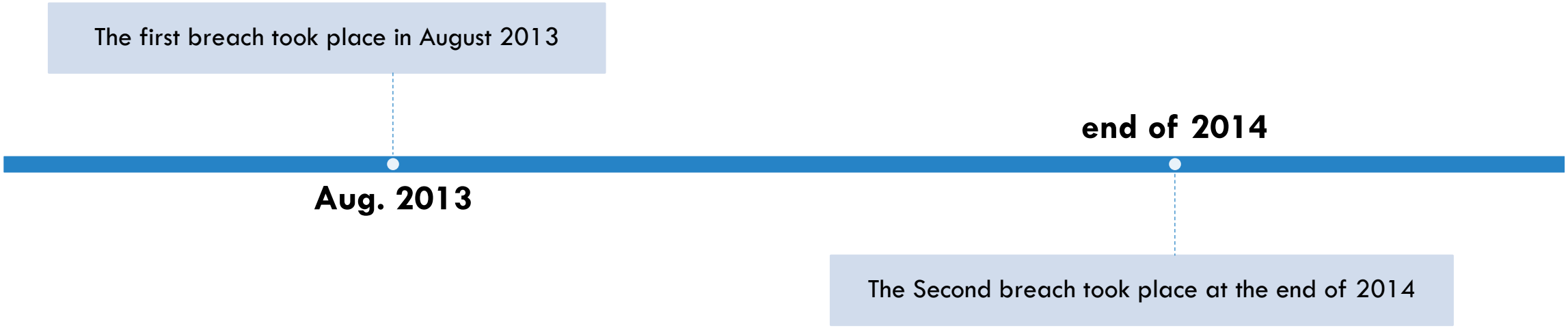
CITC 1351 025

FOUNDATIONS OF INFORMATION ASSURANCE

SPRING SEMESTER 2019

Professor GEORGE MEGHABGHAB


IDENTIFY
Asset management
Business environment
Governance
Risk assessment
Risk management strategy
PROTECT
Access control
Awareness and training
Data security
Information protection and procedures
Maintenance
Protective technology
DETECT
Anomalies and events
Security continuous monitoring
Detection process
RESPOND
Response planning
Communications
Analysis
Mitigation
Improvements
RECOVER
Recovery planning
Improvements
Communications



WHEN THE BREACHES OCCURRED

Yahoo! reports that both breaches were performed through falsified web cookies. Yahoo! at the time did not use any type of data encryption on user's security questions/answers.

HOW DID IT HAPPEN

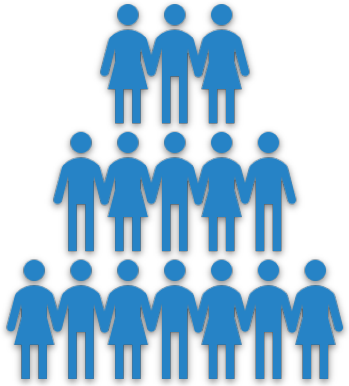
STOLEN DATA

- Names
- Usernames
- Passwords
- Security Questions/Answers
- Phone numbers
- Addresses

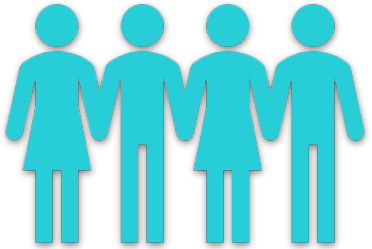
ANNOUNCEMENT OF BREACHES

The August 2013 breach was reported December 2016

The late 2014 breach was reported September 2016



In the breach of 2013
3,000,000,000 (billion) users



In the breach of 2014
500,000,000 (million) users

WHO WAS AFFECTED

THE CULPRIT

Yahoo! suspects a state-sponsored actor such as China or Russia

The U.S. Government states that the attack has similarities to previous breaches linked to the Russian Government.

Sean Sullivan of F-Secure and Kenneth Greers of Comodo both suspect China

InfoArmor believes it was the works of an Eastern European criminal gang related to Groupe E.

WHAT HAPPENED WITH THE STOLEN DATA

The data was found being sold on the dark web on a website called TheRealDeal. InfoArmor linked Group E as the source of the data being sold by a seller of the name Peace_Of_mind (aka Peace). It is also believed that the information is being sold to other web sellers as well.

The U.S. Government, who thinks the breach was performed by a nation-state, believes the attack was actually used to gain information on specific people.

LEGAL ACTIONS

The FBI officially charged four men with the breach.

Agent Dmitry Dokuchaev	Agent Igor Sushchin	Alexsey Belan (Hacker on the FBI's Ten Most Wanted list)	Karim Baratov (Canadian hacker)
•At Large	•At Large	•At Large	•5 Year Sentence •$250,000 Fine

Karim Baratov is the only one to be arrested who claimed innocent and then later pled guilty to hacking at least 80 accounts.

WHAT DID IT COST YAHOO!

VERIZON YAHOO! MERGER DEAL

Verizon was in negotiations with Yahoo! to buy a portion of their company. Their original offer was $4.83 billion

After the announcement of the breaches Verizon reduced their offer by $350 million

FINES

The U.S. Government fined Altaba, the company that holds assets of Yahoo! not purchased by Verizon, $35 million for failure to disclose the 2014 breach in a timely manner

CLASS ACTION LAWSUITS

- By November 9, 2016, there were a reported 23 lawsuits related to the late 2014 breach
- 5 were combined into one lawsuit
- Verizon and Altaba agreed to split the cost of a $50 million settlement
- They also had to provide two years of free credit monitoring through AllClear ID
- Following the August 2013 breach announcement, another class-action lawsuit was filed stating Yahoo! failed, and continues to fail, to provide adequate protection of its users personal and adequate confidential information

FOREIGN ACTIONS

Foreign countries such as Ireland, are also investigating these breaches

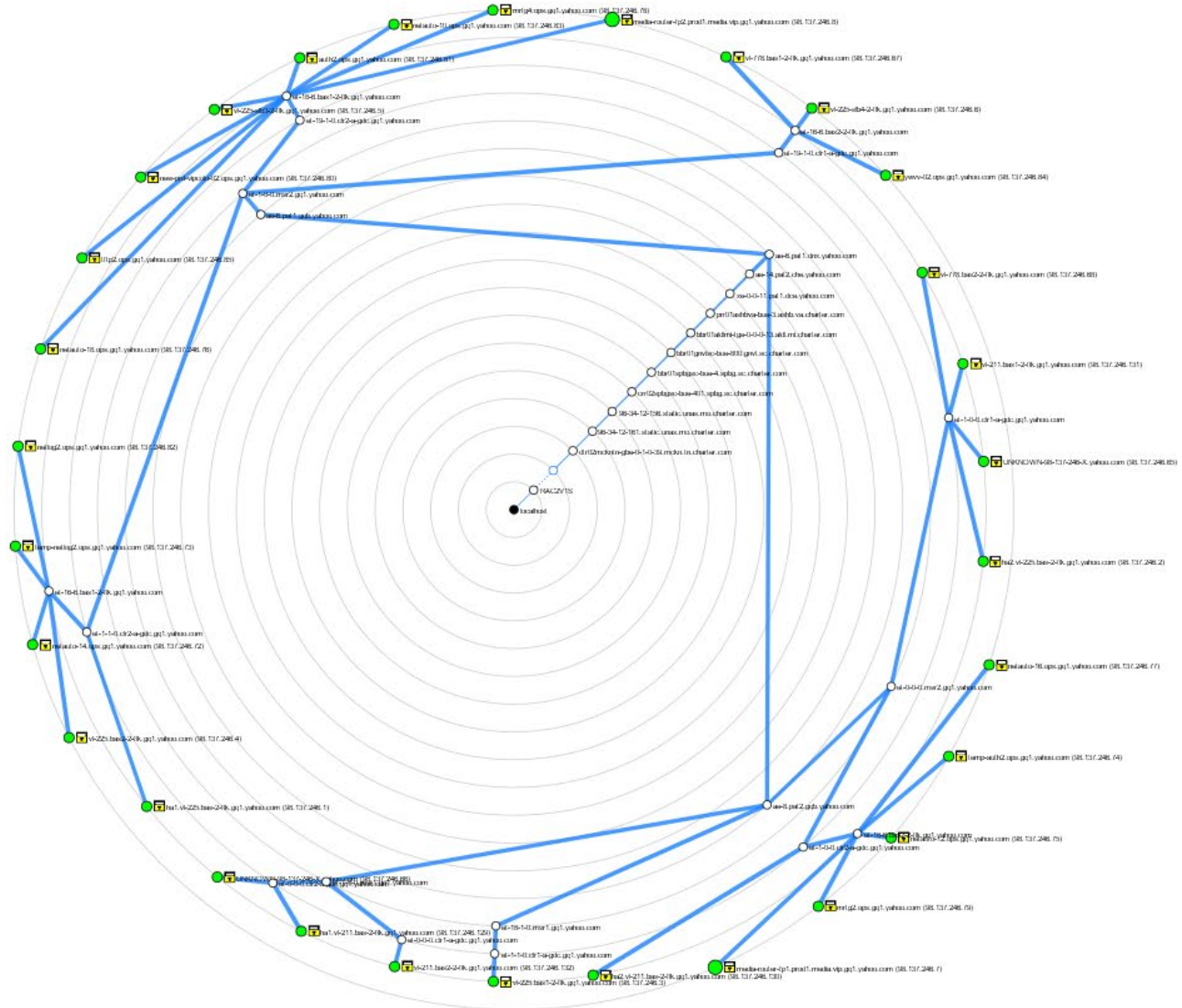
Other countries, like Germany, are recommending their government and other German users to seek out other email and internet solutions

NMAP

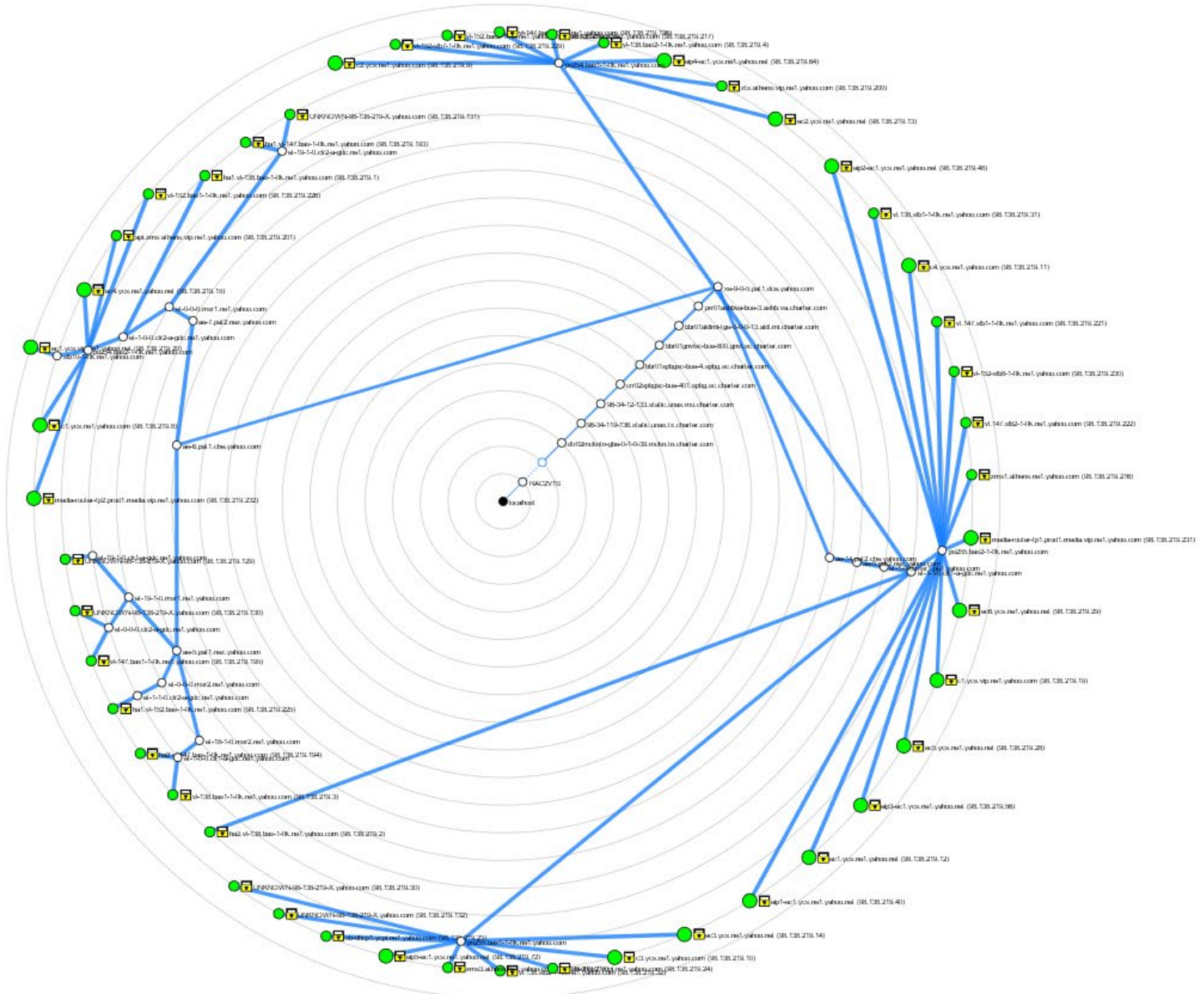
72.30.35.0/24


RAC2V1S
localhost
UNKNOWN-72-30-35-X.yahoo.com (72.30.35.66)
et-0-1-0.clr1-a-gdc.bf1.yahoo.com
ae-0.pat2.bfw.yahoo.com
UNKNOWN-72-30-35-X.yahoo.com (72.30.35.52)
vl-258.bas1-1-flk.bf1.yahoo.com (72.30.35.98)
vl-258.bas2-1-flk.bf1.yahoo.com (72.30.35.99)
UNKNOWN-72-30-35-X.yahoo.com (72.30.35.50)
UNKNOWN-72-30-35-X.yahoo.com (72.30.35.65)
vl-350.bas2-1-flk.bf1.yahoo.com (72.30.35.83)
UNKNOWN-72-30-35-X.yahoo.com (72.30.35.34)
media-router-fp2.prod1.media.vip.bf1.yahoo.com (72.30.35.10)
eth-18-3-bas1-1-flk.bf1.yahoo.com
vl-156.slb4-1-flk.bf1.yahoo.com (72.30.35.6)
ha1.vl-350.bas-1-flk.bf1.yahoo.com (72.30.35.81)
secops-proxy-02.ops.bf1.yahoo.com (72.30.35.55)
et-19-0-1.msr1.bf1.yahoo.com
et-0-1-0.clr2-a-gdc.bf1.yahoo.com
UNKNOWN-72-30-35-X.yahoo.com (72.30.35.35)
UNKNOWN-72-30-35-X.yahoo.com (72.30.35.36)
secops-proxy-01.ops.bf1.yahoo.com (72.30.35.54)
vl-156.slb3-1-flk.bf1.yahoo.com (72.30.35.5)
eth-17-3.bas1-1-flk.bf1.yahoo.com
whs-02.ops.bf1.yahoo.com (72.30.35.41)
vl-156.bas2-1-flk.bf1.yahoo.com (72.30.35.4)
96-34-12-133.static.unas.mo.charter.com
96-34-119-136.static.unas.tx.charter.com
dtr02mcintn-gbe-0-1-0-39.mcin.tn.charter.com
ha1.vl-258.bas-1-flk.bf1.yahoo.com (72.30.35.97)
t2.time.bf1.yahoo.com (72.30.35.88)
media-router-fp1.prod1.media.vip.bf1.yahoo.com (72.30.35.9)
t1.time.bf1.yahoo.com (72.30.35.89)
eth-17-3.bas2-1-flk.bf1.yahoo.com
UNKNOWN-72-30-35-X.yahoo.com (72.30.35.51)
whs-01.ops.bf1.yahoo.com (72.30.35.40)
UNKNOWN-72-30-35-X.yahoo.com (72.30.35.67)
vl-156.bas1-1-flk.bf1.yahoo.com (72.30.35.3)
UNKNOWN-72-30-35-X.yahoo.com (72.30.35.68)

98.137.246.0/24



98.138.219.0/24



SOURCES

https://en.wikipedia.org/wiki/Yahoo!_data_breaches