

**RSA**®Conference2018

San Francisco | April 16–20 | Moscone Center



#RSAC

SESSION ID: TV-W07

# MY FIRSTHAND EXPERIENCE WITH RANSOMWARE

**Birat Niraula**

Manager, Cyber Security  
Capital One  
@biratniraula

# Agenda



- Ransomware
- Common Ransomware Attack Vectors
- Some of recent Ransomware attacks
- Discussion on my first-hand experience with Ransomware
- Short-term and Long-term effects
- Potential solutions for prevention and cure
- Looking back
- Summary

# Ransomware



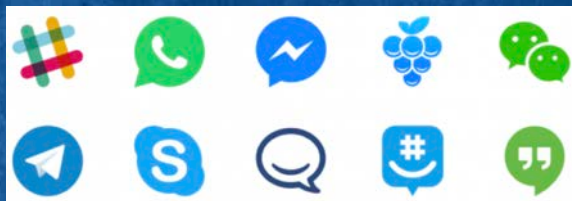
- A type of malware that prevents user from accessing their system by locking the system's screen or files unless ransom is paid
- Motivation for creating Ransomware
- Entities creating Ransomware
- Ransomware targets
- Ransomware-As-A-Service



# Common Ransomware Attack Vectors



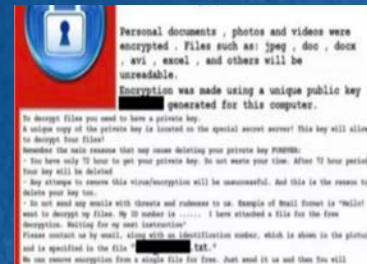
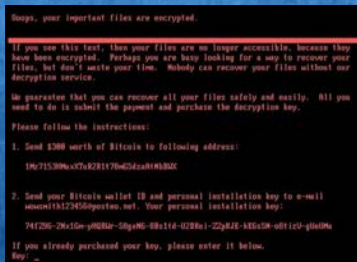
- Email attachments and URLs
- Online ads
- Unsecure websites
- Downloads
- Instant Messages
- Cloud based collaboration tools



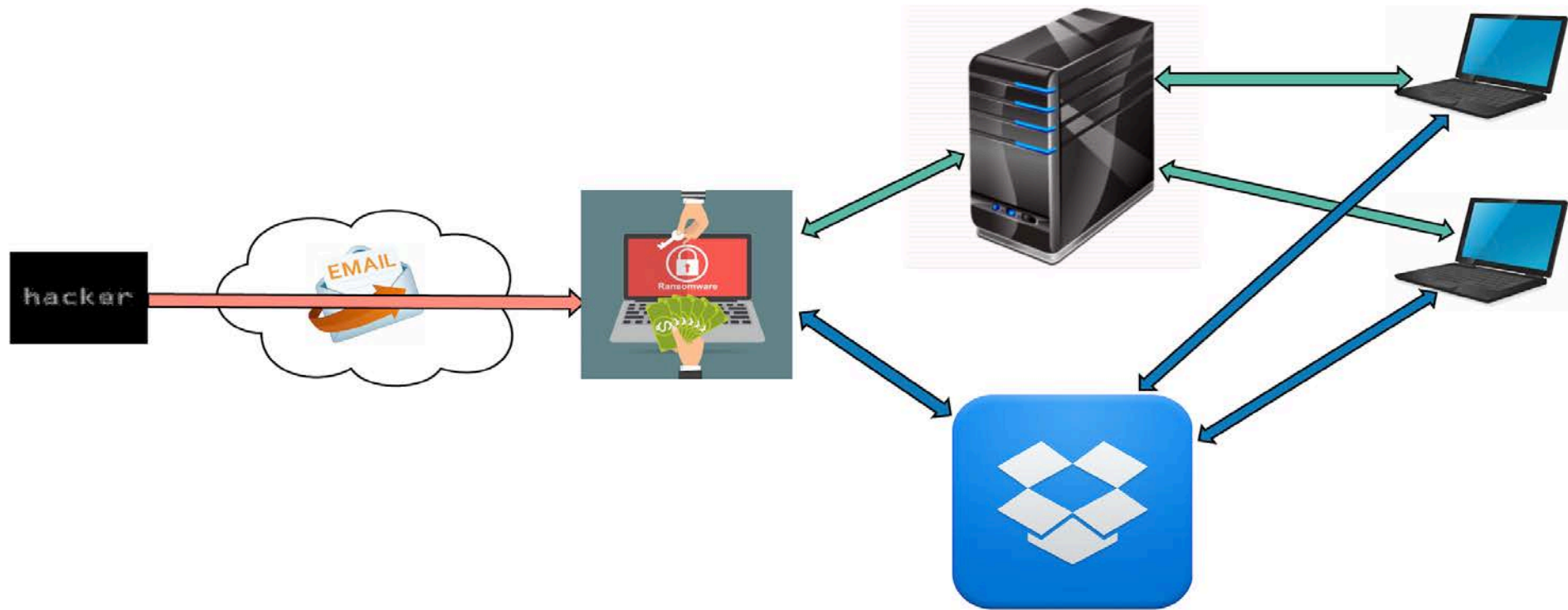


# Some of recent Ransomware attacks

- WannaCry
- NotPetya
- BadRabbit
- Locky
- Cerber
- CrySis



# Discussion on my first-hand experience with Ransomware



# Short-term and Long-term effects (contd)



- PANIC



- Argument



- Plan



- Control



# Short-term and Long-term effects



- Lessons learned



- Investment in Security



- Investment in Employee and Training



- Table tops





# Potential solutions for prevention and cure



- “Prevention is better than Cure”
- Prevention
  - Patching, Backups, Disable macros, MS Office viewer, User awareness, User access/privilege limitation, Network Segmentation, Prevention apps, etc.
- Cure
  - Do not Panic, Training, Task force, Train and practice, Contain, Recover, Lessons learned, Train again, etc.

# Looking back



- Once in a life time (hopefully)
- Should have been better prepared
- Training
- Task force
- Security Solutions

# Summary



- Ransomware are common
- Training and awareness
- Be prepared
- Get everyone involved