The Evolution of Ransomware and its Mitigation Strategies

Ariel Cordes
UMN-Morris Computer Science Senior Seminar
April 18 2020

Or: Know Thy Enemy and Know Thyself

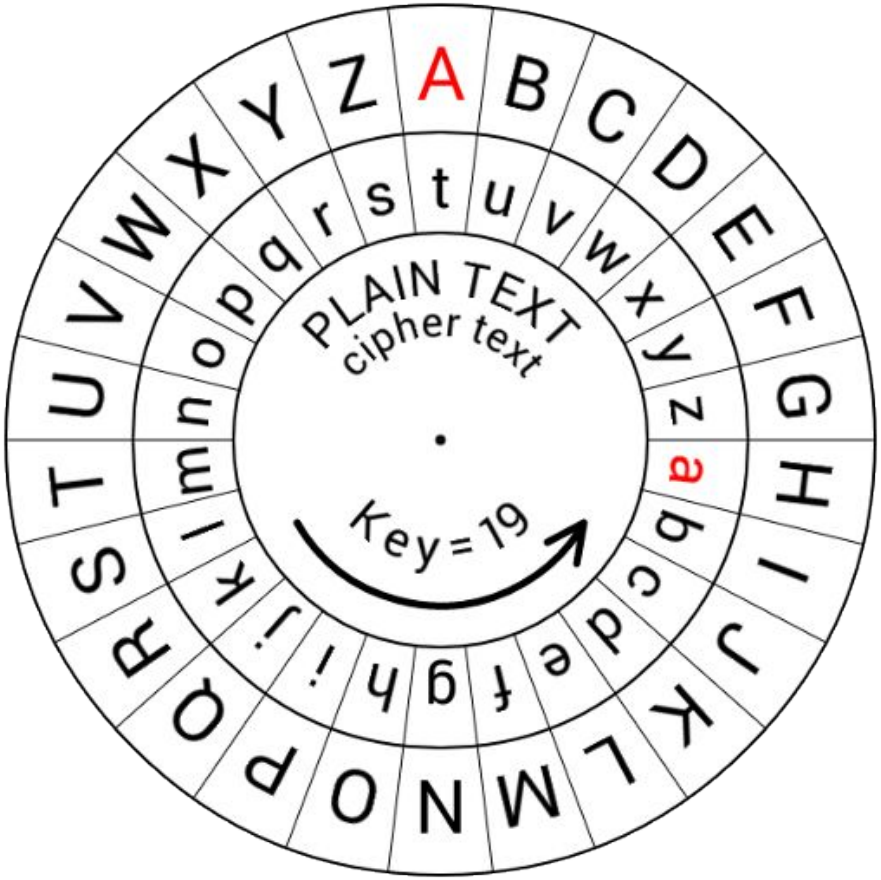
(Ransomware is thy enemy)

Background

Encryption

What is encryption?

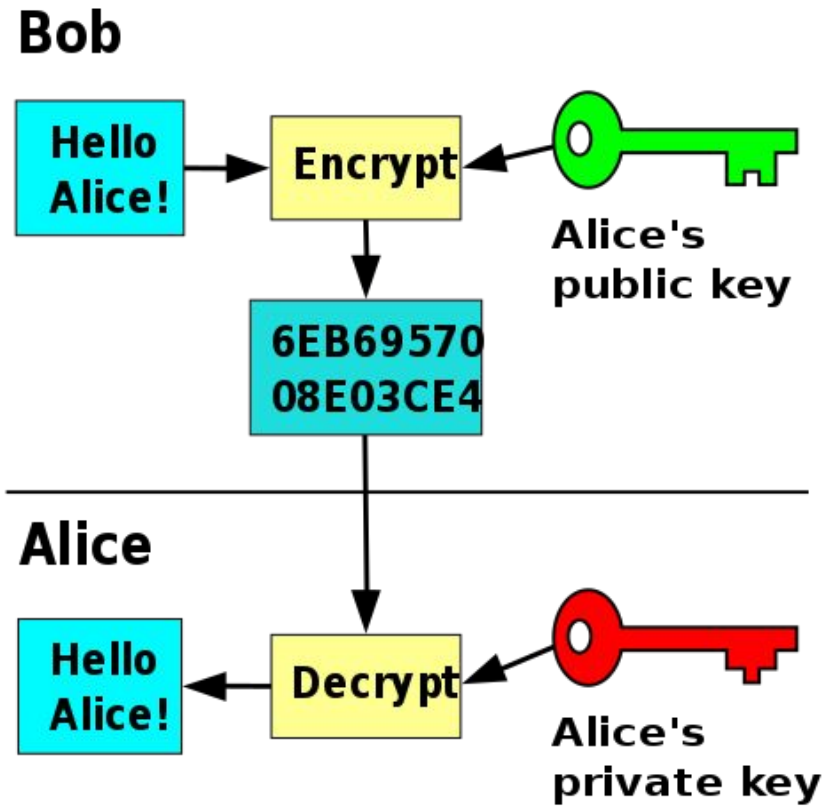
Why do we care?



Symmetric vs Asymmetric Encryption

What is symmetric encryption?

What is asymmetric/public-key encryption?



What is Malware?

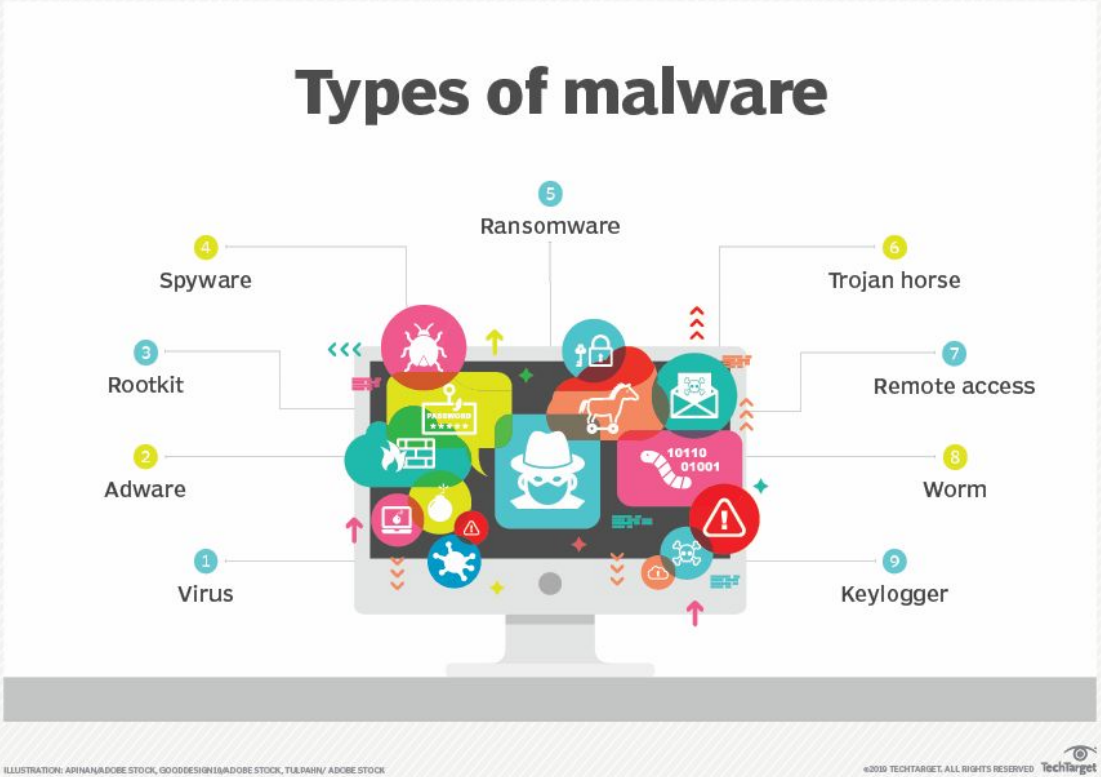
(Don’t hurt me…

Don’t hurt me….

No more…)

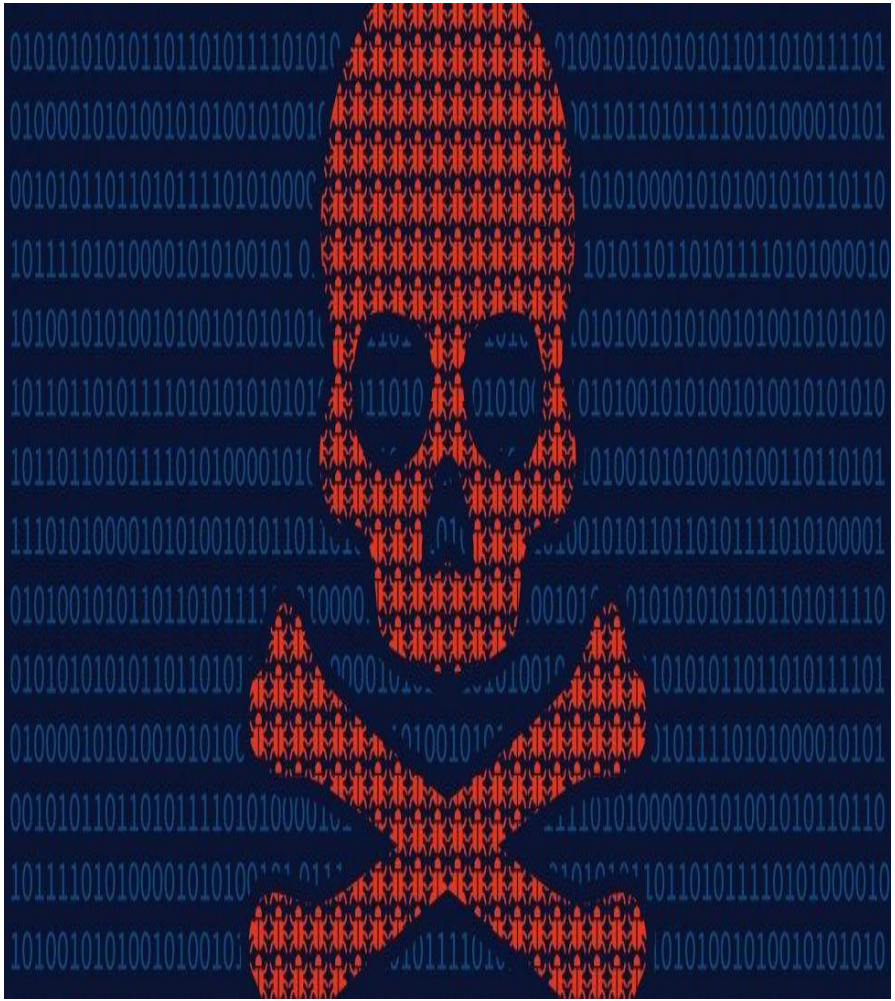
Malware

What is malware?



Command and Control Server

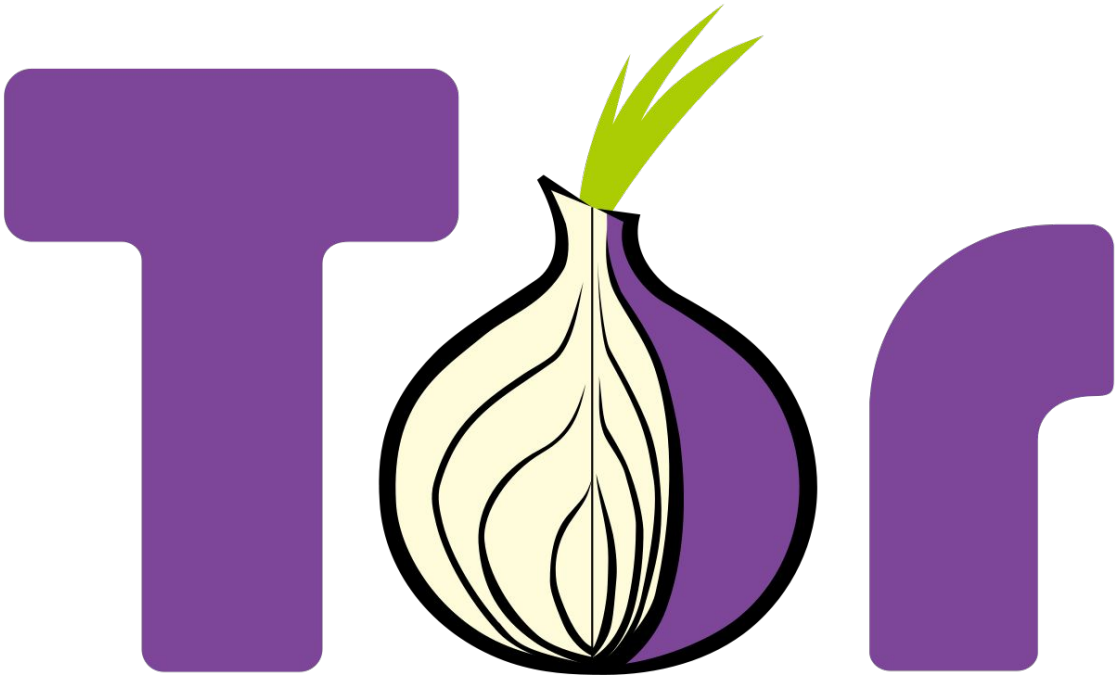
What is a command and control server?



Tor

What is Tor?

(Like onion...)

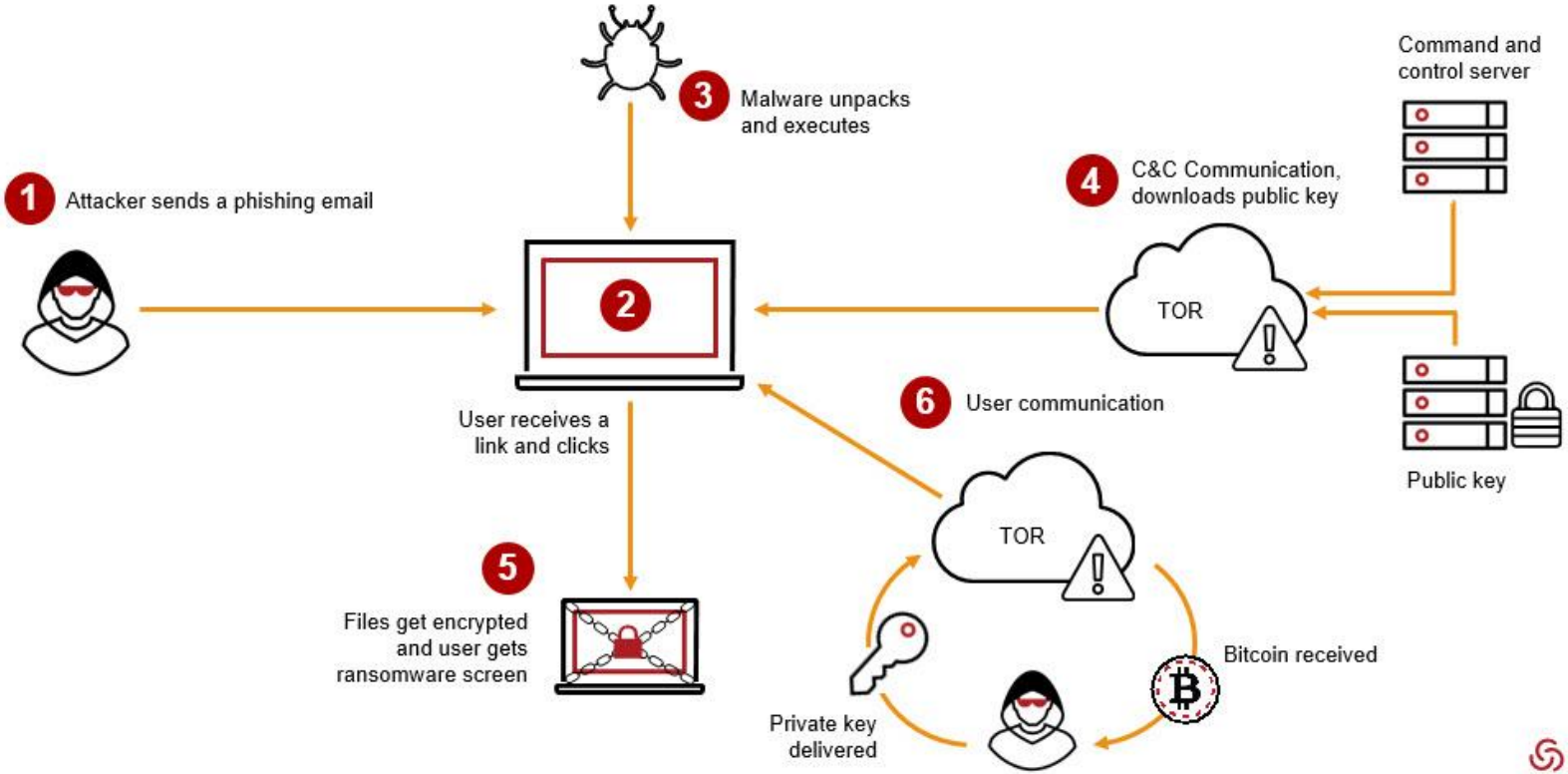


Ransomware

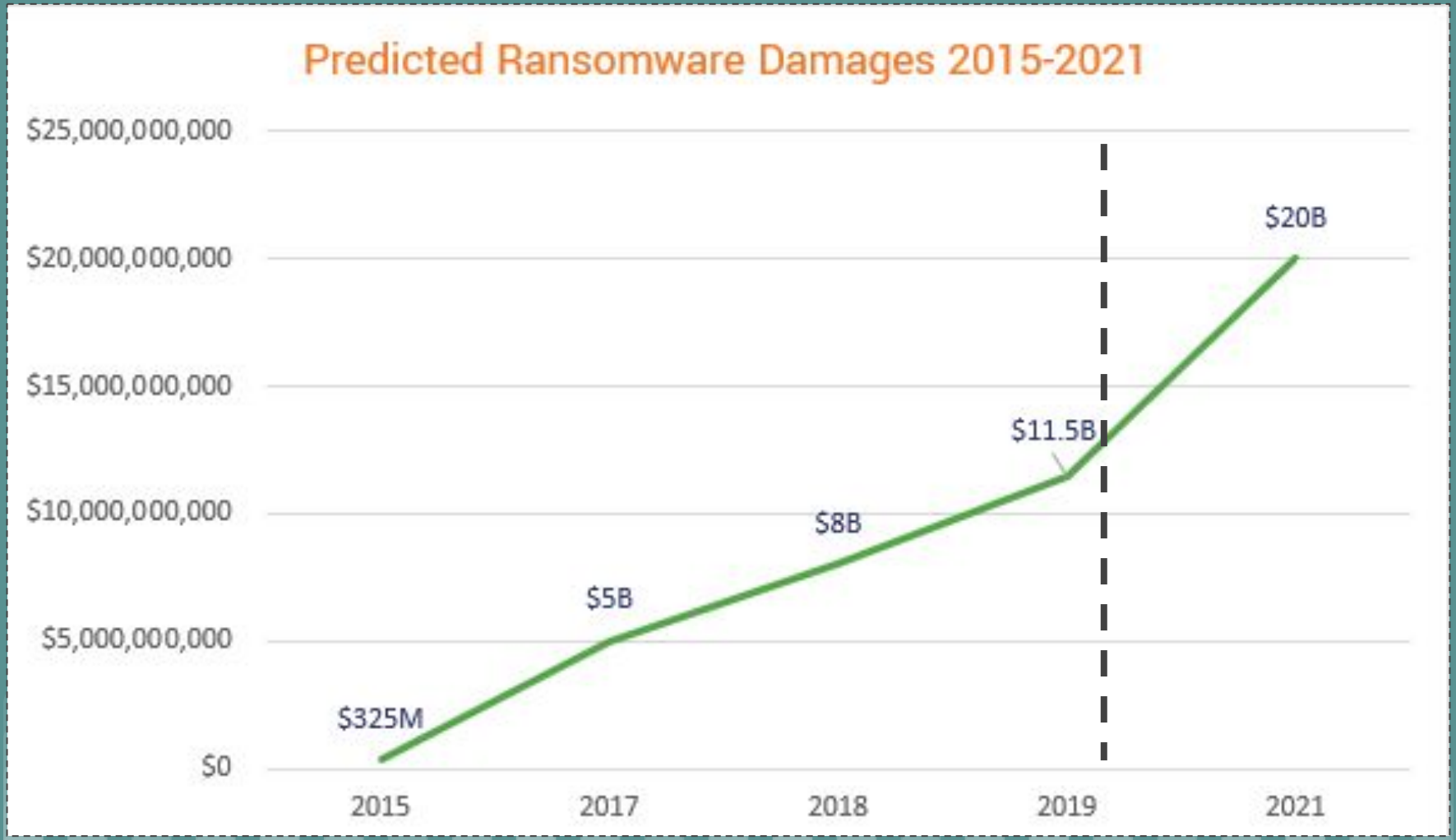
What is Ransomware?

- Malicious software (Malware)
- Blocks access to users' files
- Claims to restore files upon payment ("ransom")

The Anatomy of a Ransomware Attack

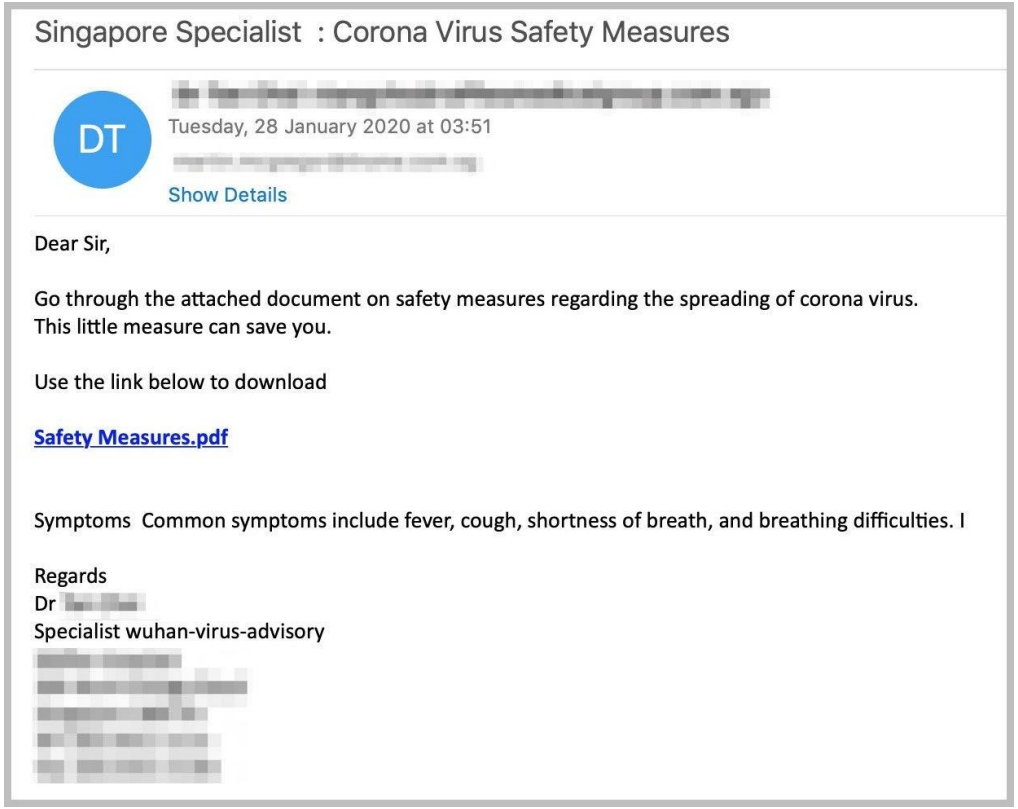


Centrify
ZERO TRUST PRIVILEGE


Predicted Ransomware Damages 2015-2021
$25,000,000,000
$20,000,000,000
$15,000,000,000
$10,000,000,000
$5,000,000,000
$0
$325M
$5B
$8B
$11.5B
$20B
2015
2017
2018
2019
2021

Phishing Email + Link Click

- Why email?
- How does it work?
- How to prevent?



Singapore Specialist : Corona Virus Safety Measures

DT

[redacted]

Tuesday, 28 January 2020 at 03:51

[redacted]

Show Details

Dear Sir,

Go through the attached document on safety measures regarding the spreading of corona virus.
This little measure can save you.

Use the link below to download

Safety Measures.pdf

Symptoms Common symptoms include fever, cough, shortness of breath, and breathing difficulties. I

Regards
Dr [redacted]
Specialist wuhan-virus-advisory
[redacted]

Unpacking and Executing

- How does it work?
- How to block it?

Command and Control Server Communication

- Cryptographic key acquisition

- How to block?

Encryption of Files

- What gets encrypted?
- How to break

User Communication

- Sending payment
  - Via cryptocurrency
- How to block
  - Don’t send payment

So What?/Conclusions

- Ransomware isn’t going away
- Need strong defenses

Questions?


WHAT?
WHY?
WHERE?
WHEN?
WHO?
HOW?
WHICH?
WHOSE?
WHAT? HOW? WHY?
WHO? WHERE? WHAT? HOW?
WHY? HOW? WHERE?
WHO? WHOSE?
WHERE? WHICH? WHOSE? WHEN? WHY?
HOW? WHO?
WHAT? HOW? WHY?
WHERE? WHAT? HOW?
HOW?

Acknowledgements

Peter Dolan — Advisor

KK Lamberty — Senior Seminar Instructor

Kevin Arhelger — Alumni Paper Reviewer

Charlot Shaw — Presentation Feedback

Citations

https://blogs.forbes.com/louiscolumbus/files/2019/07/Anatomy-of-a-ransomware-attack.jpg

https://www.thesslstore.com/blog/ransomware-statistics/#ransomware-statistics-the-costs-of-ransomware-attacks

https://cdn.ttgtmedia.com/rms/onlineimages/whatis-malware_types.png