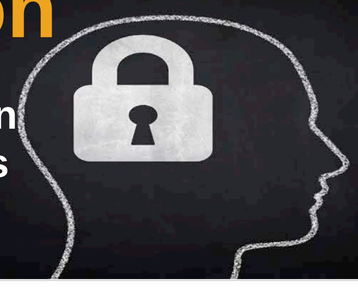
Ransomware: Recommendations against the Extortion

Shubham Goel, Graduate Student at School of Information Sciences, University Of Illinois Urbana Champaign
Advisor- Dr. Masooda Bashir, School of Information Sciences/Information Trust Institute, University of Illinois Urbana Champaign



Background

- Ransomware is form of a malicious software which holds the individual's computer or company's information system hostage until the ransom amount is being paid.
- The motive for ransomware attacks is monetary unlike other types of attacks, it encrypts files so that they cannot be accessed and the victim is notified that an exploit has occurred and is given instructions to decrypt the file.
- FBI has estimated that ransomware is a billion dollar industry in 2016 and every hour 4000 computers get affected by ransomware.
- Fig 1 shows an example of ransomware propagation.

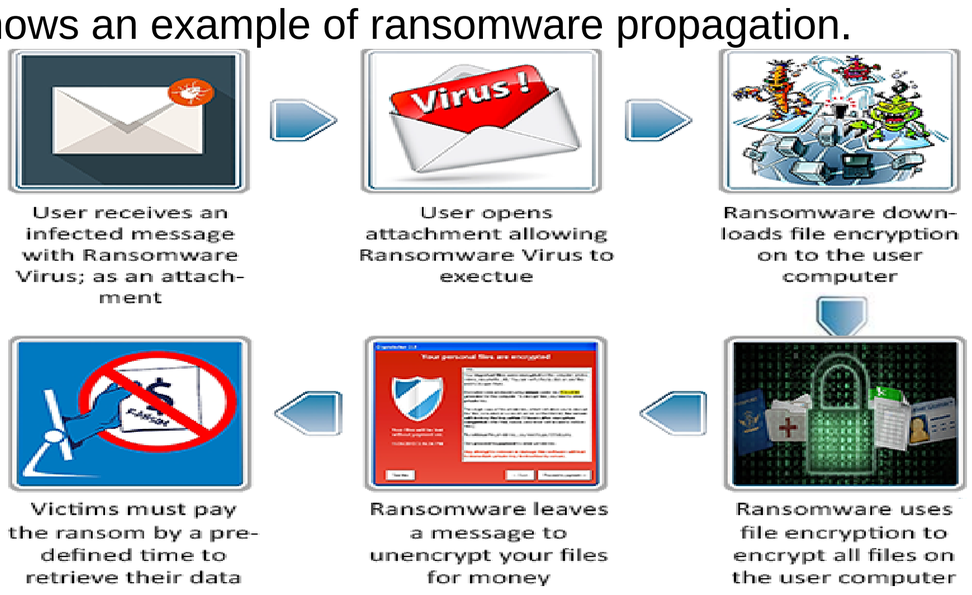


Fig 1- Ransomware Lifecycle : Image from Algosec's blog

Goals/Fundamental Questions

•The goal of this project is to distinguish the differences between various sector reports and highlight all the technical and business recommendations that are being suggested.

•Although ransomware is not a new form of malware, there is a lack of comprehensive guide for a company or an individual to be prepared against ransomware or take actions whenever confronted with an attack.

Research Method

•Identified and analyzed 49 reports from companies /government/agency/news media that were publicly available.

•The reports included in the research are threat advisories, guides, recommendations that were published in 2016-17. All reports analyzed used English as their medium.

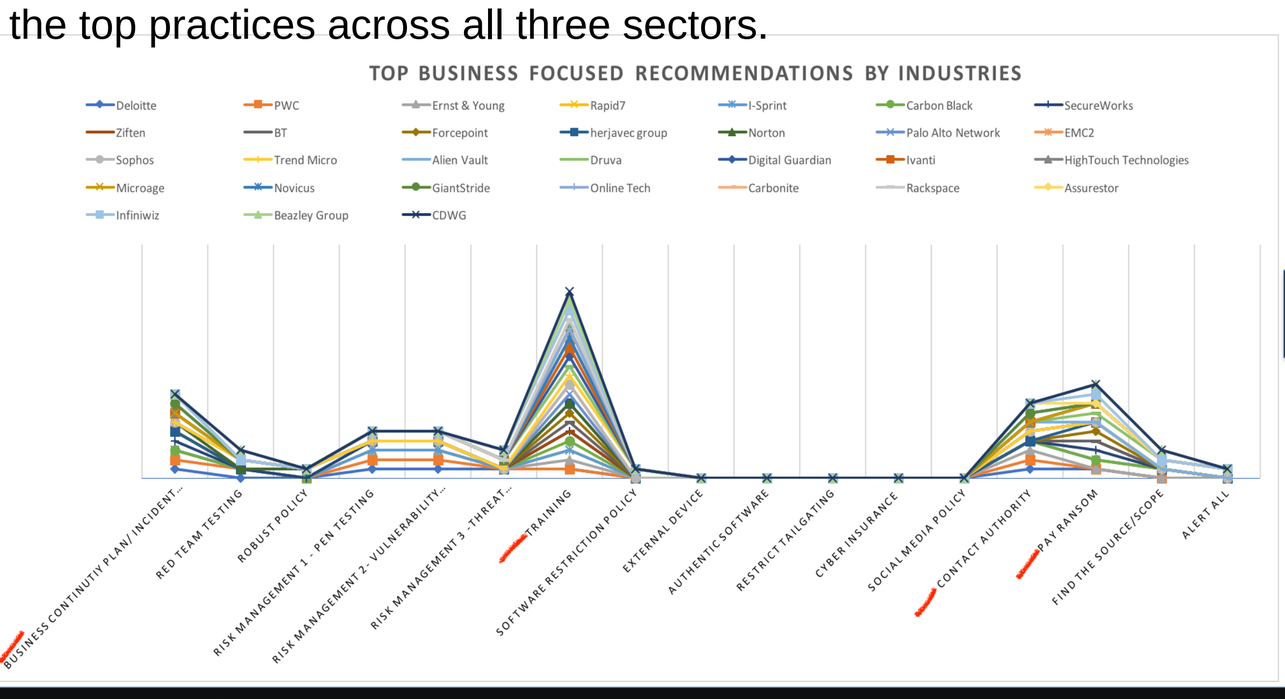
•Categorized the reports into three sectors i.e.1) Government 2)Industry 3)Online Community/Research/News Media.

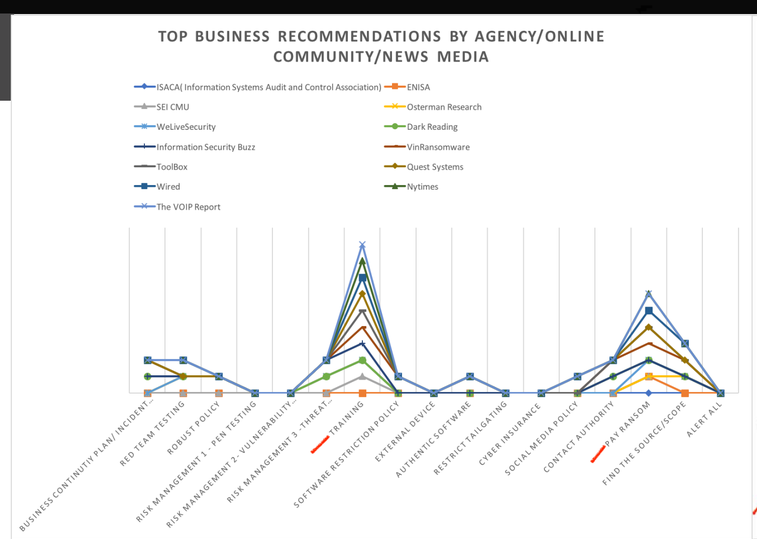
•Based on our assessment, we identified 59 factors that were recommended. Backup, Antivirus, business continuity plan are among some common practices shown in fig 2 and 3.

•Identified the similarities and differences among the reports in order to determine the best recommended practice.

Results

• Analysis of the reports shown in Fig2 displays top business focused practices in which training and ransom payment is among the top practices across all three sectors.





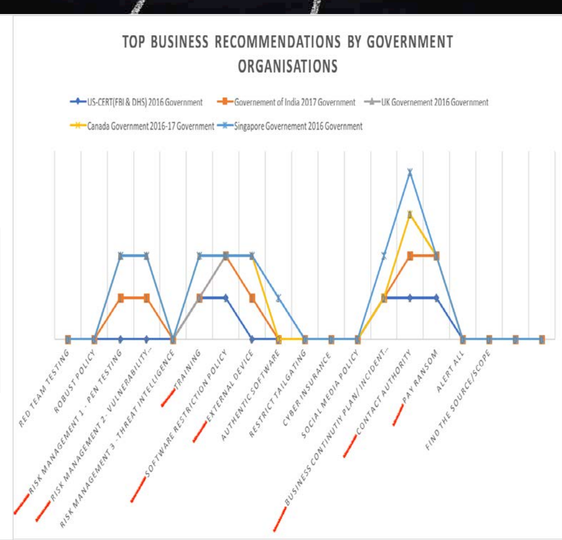
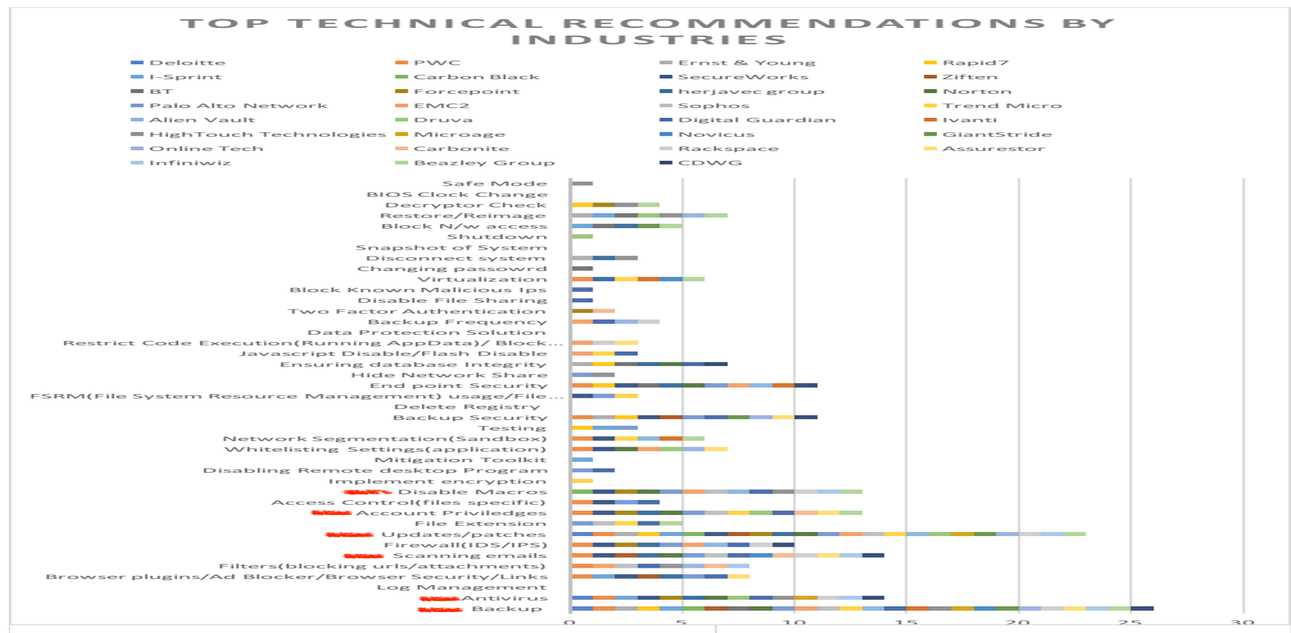
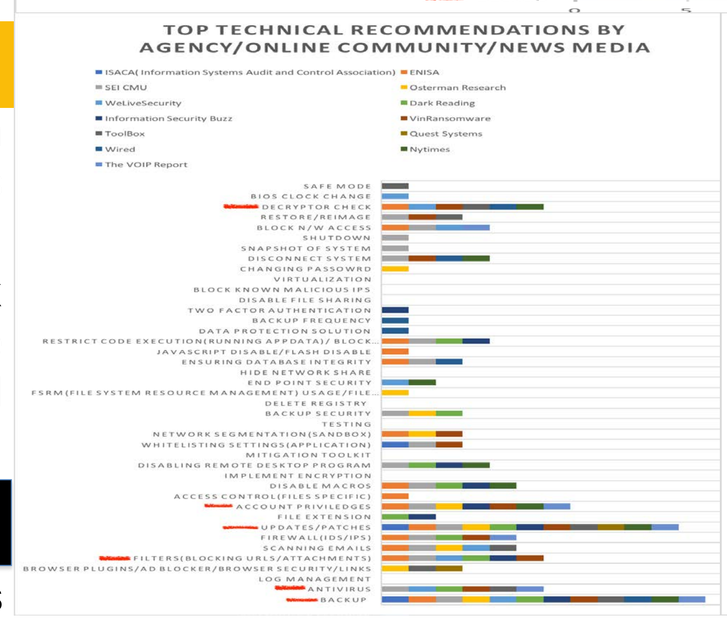


Fig 2, Top Business Recommendations





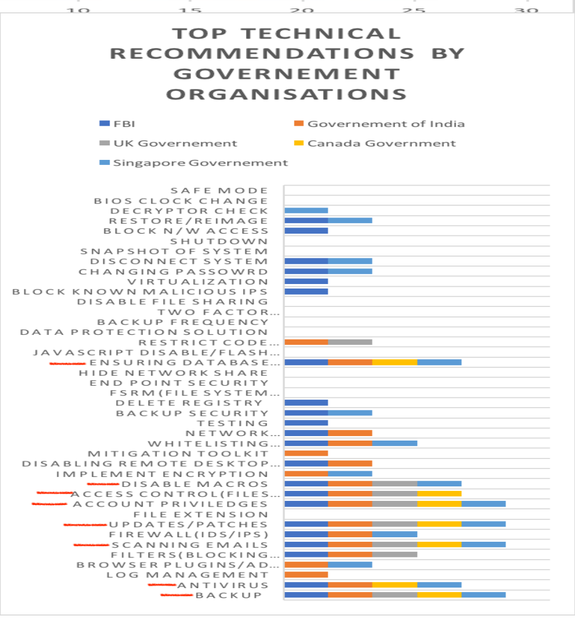


Fig 3, Top Technical Recommendations

•Fig 3 shows technical recommendations with backup, antivirus and account privileges as common suggestion.

•Our evaluation reveals that there is no single way of protecting your business or an individual through a single practice. Process of protecting against ransomware requires a set of practices that should be followed over a period of time to provide an optimal solution against ransomwares.

•In addition, our investigation reveals that the most common techniques used for infecting computers according to all the reports are spam emails, drive-by downloads, malvertising campaigns and ransomware as a service(Raas).

Limitations

- Lack of scholarly papers that are published about ransomwares.
- Although majority of the reports were published in English, there were few government reports that were published in their native language with few government website having password protected files and hence could not be included.

Future Work

•There are different ransomware families and their method of propagation is different, so it would be really helpful to various families and different practices against them.

•What are the most common reasons that companies/individual get affected?

•Separating the pre and post attack strategies.

SCIENCE OF SECURITY
VIRTUAL ORGANIZATION
Funded by the National Security Agency.

INFORMATIONTRUST INSTITUTE