Data Security: The Texas Identity Theft Enforcement and Protection Act and Other Considerations

Presented by:

D. Esther Chavez
Adrian P. Senyszyn

DISCLAIMER & FAIR USE NOTICE

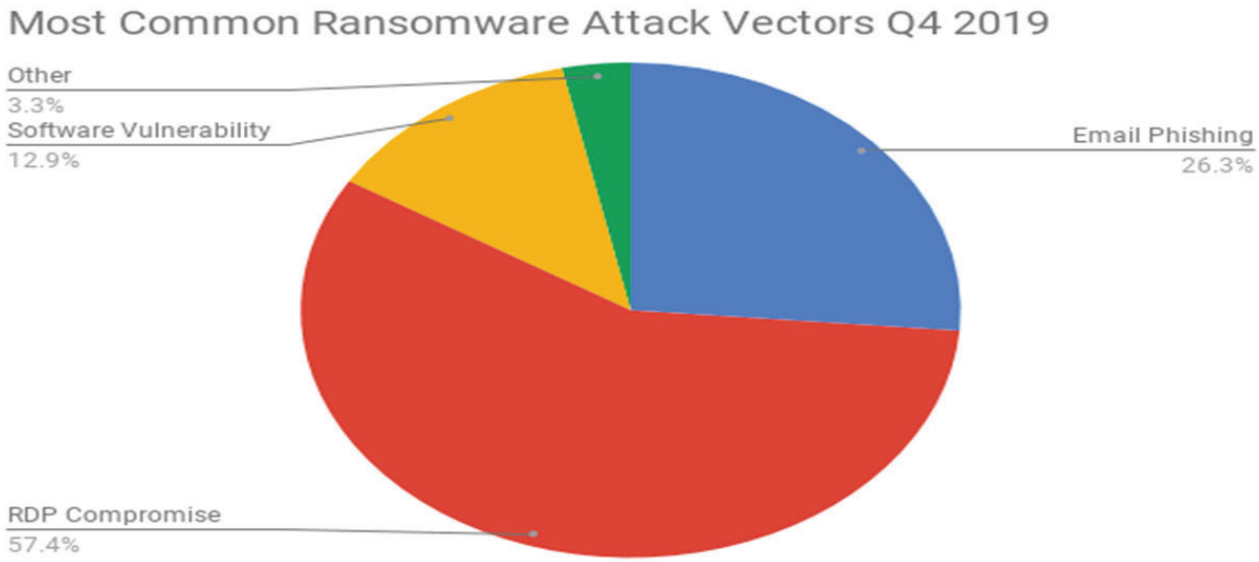
- **All content in this slide show and all statements and opinions made during the presentation are those of the speakers and not of the Texas Attorney General's Office or MehaffyWeber, P.C.**
- **This presentation was created and intended for non-profit educational use only. It is not intended for, and it should not be used for, any commercial use.**
- **This presentation may contain content and images not authorize for use by its owner. These presenters believe the use of any such material constitutes "fair use" as provided by Title 17, Section 107 of U.S. Copyright Law.**

Federal Bureau of Investigation
Internet Crime Complaint Center(IC3)

Ransomware attacks are becoming more targeted, sophisticated, and costly, even as the overall frequency of attacks remains consistent. Since early 2018, the incidence of broad, indiscriminant ransomware campaigns has sharply declined, but the losses from ransomware attacks have increased significantly, according to complaints received by IC3 and FBI case information. Cyber criminals use a variety of techniques to infect victim systems with ransomware. Cyber criminals upgrade and change their techniques to make their attacks more effective and to prevent detection. The FBI has observed cyber criminals using the following techniques to infect victims with ransomware: Email phishing campaigns, Remote Desktop Protocol vulnerabilities, and Software vulnerabilities.

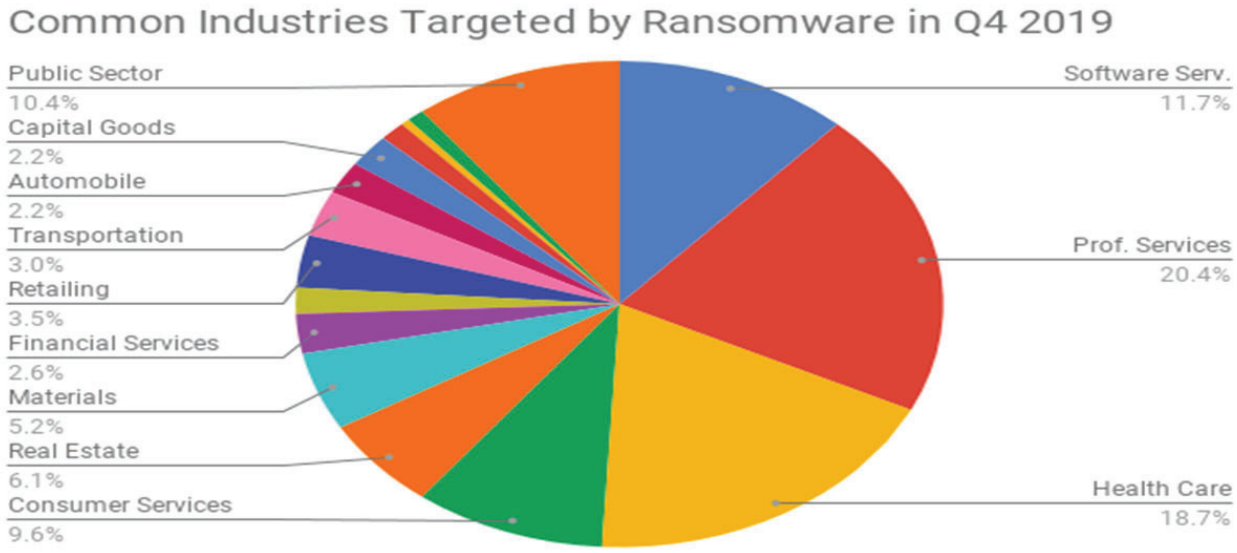
Source: FBI Oct. 2, 2019, Alert No. I-100219-PSA
https://www.ic3.gov/media/2019/191002.aspx

3



Source: Coveware Blog Jan. 22, 2020
https://www.coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate

4



Source: Coveware Blog Jan. 22, 2020
https://www.coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate

5

May 15, 2020

Grubman, Shire, Meiselas & Sacks said in a statement Friday that law firms have not been immune to escalating attacks by foreign cybercriminals.

“Despite our substantial investment in state-of-the-art technology security, foreign cyberterrorists have hacked into our network and are demanding $42 million as ransom," it said. "We are working directly with federal law enforcement and continue to work around the clock with the world’s leading experts to address this situation.” ~ NBC News

Source: NBC News, May 15, 2020, by Kevin Collier and Diana Dasrath
https://www.nbcnews.com/tech/security/criminal-group-hacked-law-firm-threatens-release-trump-documents-n1208366

6

Title search: Data Security: The Texas Identity Theft Enforcement and Protection Act and Other Considerations

First appeared as part of the conference materials for the
15th Annual Advanced Texas Administrative Law Seminar session
"Data Security: The Texas Identity Theft Enforcement and Protection Act and Other Considerations"