

Mat-Su Borough

2018 Cyber Attack



- What Happened
- Why It Happened
- The Response
- Going Forward

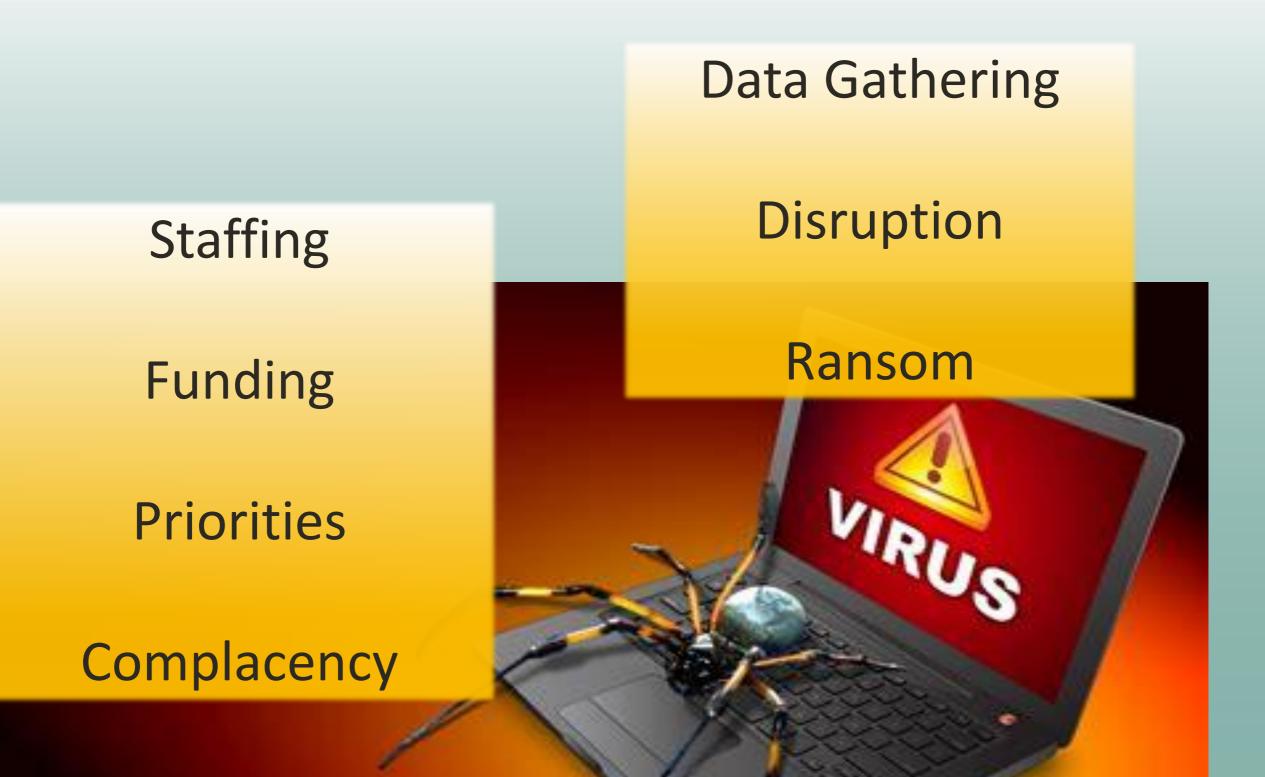
Zero Day

- Late April eMail phishing
- Late May heavy activity
- June dormant
- July Discovery and Crypto-Locked Theoretical



- EXPLOIT **Trojan-Emotet**
 - **Credential Stealing Dridex**
 - **PowerShell Empire**
 - **Ransom Ware BitPaymer**

Why It Happened



Response

Incident Response

Vendors

Volunteers

Project Management

Long hours

Emergency funding

Minimum Viable Product (MVP)

Take Care Of Your Users Communication Communication COMMUNICATION

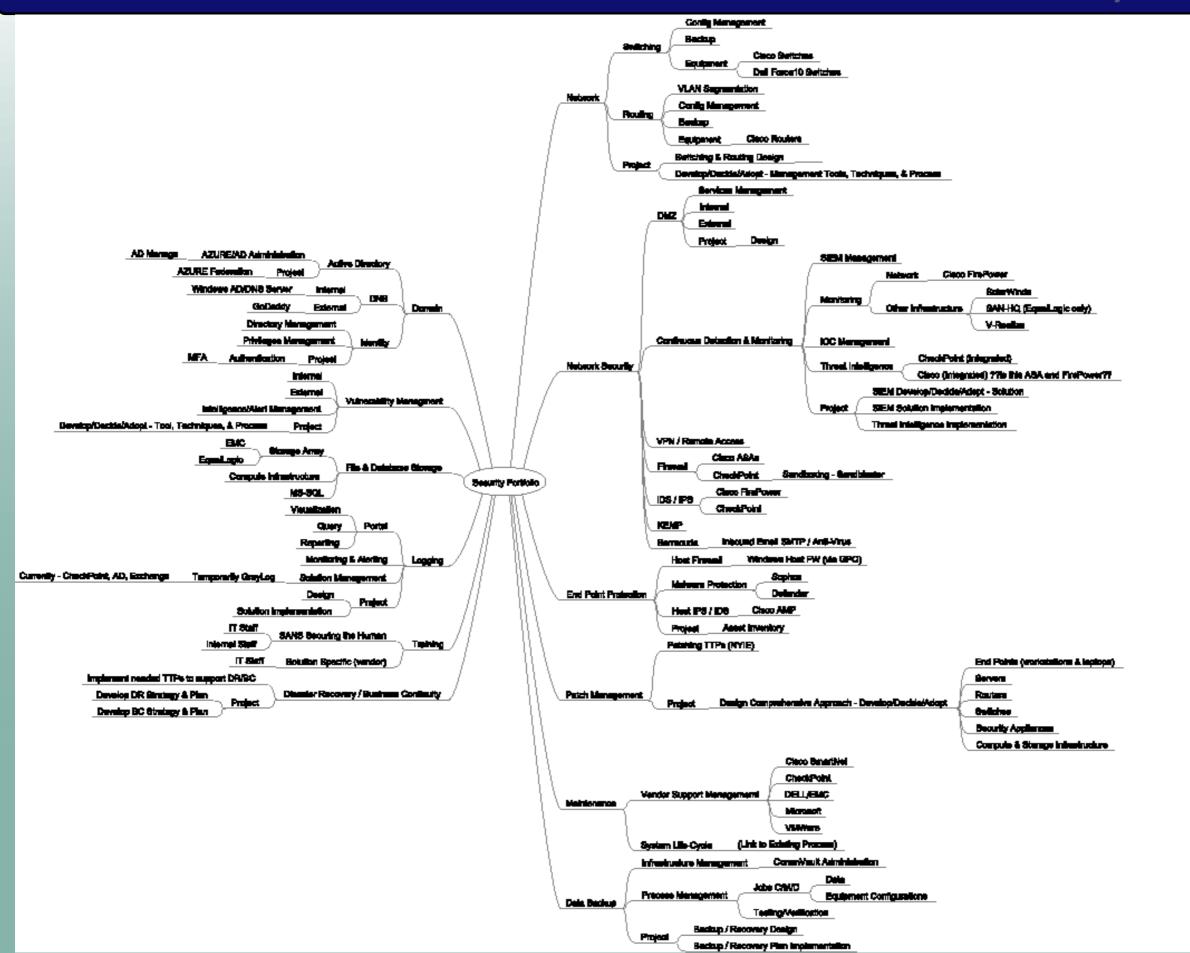
Communication Communication COMMUNICATION

Partnering

Federal State Local Commercial MS-ISAC DHS – US Cert InfraGard CIO Council Smart Community Forum

Take Care OfEach OtherWe Can't Do This Alone

Security Portfolio



Discussion

