Berkman Ce b6169

Berkman Center 27 Apr 2017 Healthcare Ransomware

Berkman Center 27 Apr 2017 Healthcare Ransomware

- your medical record is worth more to hackers than your CC

▾ huge increase in # of medical records breached

- 2010 less than 10M
- 2015 80m
- however, the price per record on black market is dropping significantly
- why is it more difficult to secure health care data than CC's?
- ransomware more significant threat now

▾ issues on understanding the risk

- not obligated to report
- hospitals not incentivized to talk about it

▾ strains of ransomware specifically designed for hospitals

- often tied to ransom requests in bitcoin.
- newer strains are even more targeted and increasing price of ransom (like Lockie)
- market is balancing out around $25k payouts

▾ infection chain

▾ often email and attached documents

- training is pretty robust at hospitals, but volume of legit and illegit attachments skews awareness
- often a hook to enable macros to do the encrypt
- often detailed instructions (even w/ call centers!) on how to free up your encrypted files
- bitcoin was an enabler for more anonymous payments
- note: lockie is even goes after the auto created shadow copies

▾ why hospitals?

- legacy systems

- heavy relaince on 3rd party systems and consultants for iT
- urgent need for access to info and continuity of service

- ▾ complete lack of criminal ethics
- ▾ note: there are ethics debates w/in ransomware community on a few points:
    - whether hospitals are a legitimate target
    - whether to actually decrypt upon payment (honor amongst thieves)
- ▾ what guidance is emerging in the policy space re: how to respond?
- ▾ Dept HHS guidance in July 2016 was pretty vague but ...
    - default presumption that a ransomware infection does represent a HIPAA breach and, therefore, subject to breach reporting provisions as outlined by HIPAA
    - if you pay, considered a breach
    - if you can fully restore the entire data set and prove no modification and no exfiltration, then no need to report the breach
- ▾ Note: the Eirie County Medical Center breach WAS ransomware
    - they decided not to pay, shutdown all systems
- ▾ still recovering 3 weeks later
- ▾ this week: getting bed coordinating back online
    - new email hospital system
    - give doctors ability to view outpatient electronic medical records (EMR)
- ▾ next week
    - electronic transmisison of radiological images
    - restoration of desktop computers
    - restoration of inpatient EMR
    - physician documentation
    - almost everything has been handled on paper and manually
- ▾ recovery cost to victim per stolen record
    - healthcare is most costly at $355 per record
    - education is 2nd highest at $246
    - financial is 3rd at $221

▾ some sentiment that:

- wake-up call that security training and heavy infosec was worthless
- almost refreshing that doctors could revert back to paper and focus on quality care

#learning/conferences