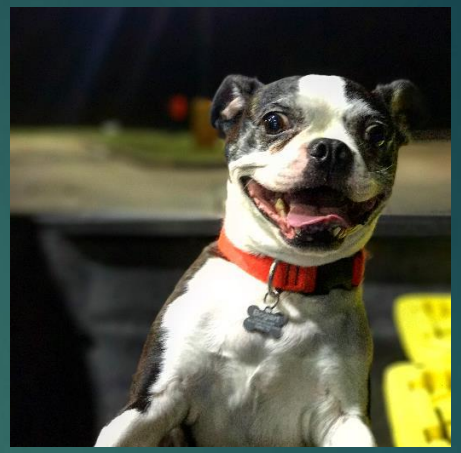
The Pulse of Cyber Security

About Me



Clayton Darnell, CISSP

- In information security for 10+ years
- Experience from defense manufacturing, restaurant, security consulting and telecom industries
- BS in Information Security
- Two adorable dogs

My opinions are solely my own and not representative of my employer

These are not regulatory or legal recommendations. Should be considered best practices

Goals!

- Overview of current events
- Review risk and impact
- Homework

Agenda

- Definitions!
- What has changed?
- Worst case scenarios are real!
- Using history to look forward
- Sec_rity is incomplete without U!
- Questions?

Definitions!

Ransomware

- A type of malware that threatens to block access to user's data unless a ransom is paid.

Malware

- Software that is intended to damage or disable computers and computer systems.

Data Breach

- Data has potentially been viewed, stolen or used by an individual unauthorized.

Exploit

- Software designed to take advantage of a flaw in a computer system, typically for malicious purposes such as installing malware.

What has changed?

- Malware grows more destructive
  - CryptoWall – 2015 - email delivered ransomware
  - Locky – Q1 2016 – email delivered ransomware
  - SamSam – Q1 2016 – spread through backdoors in web applications
  - WannaCry – Q2 2017 – spread over the internet
  - NotPetya – Q2 2017 – Targeted cyber-attack on Ukraine
- Cyber Attacks in healthcare are leading to full stop of operations.

Merck @Merck · Jun 28
Providing an update on global hacking of computer network:

Our computer network was compromised on
as part of a
organizations
IT systems as a
problem a
continuity

To meet patie
maintain a su

We believe we h
on recove
We also are
agenc

As we addre
we will con
patients, our

Nuance Healthcare
@NuanceHealth

hcare Custor
p you inform
nake regular

re:
ner Update

k through the incident imp

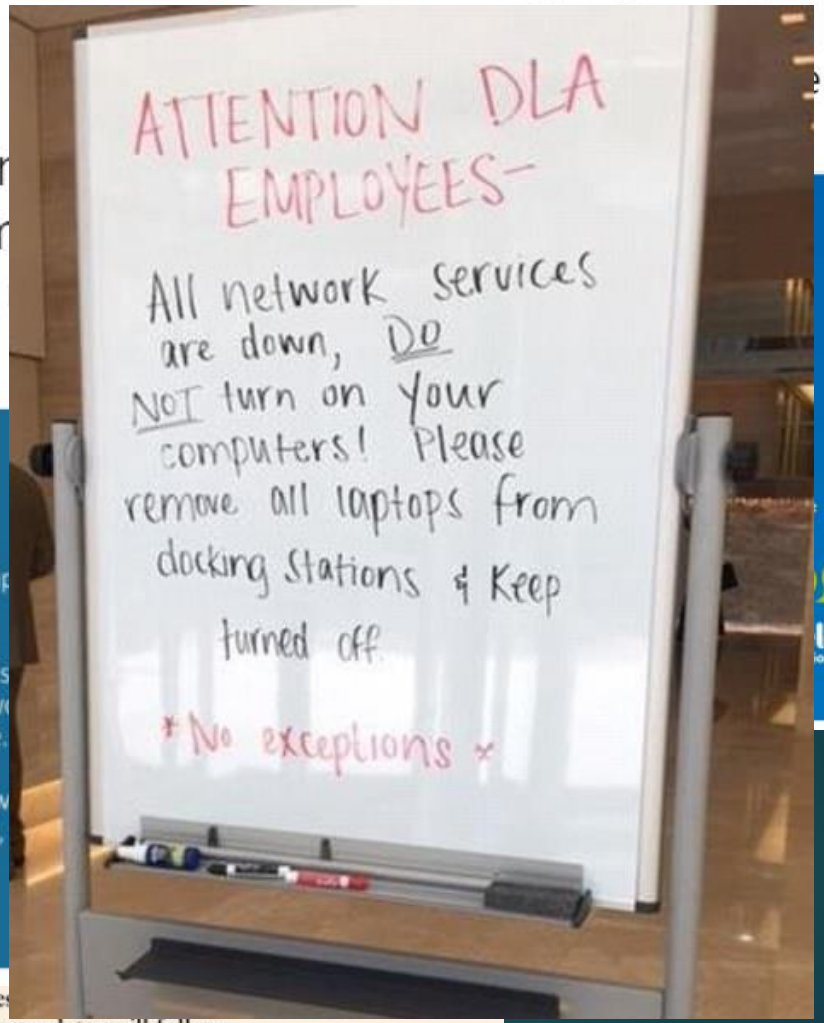
cted by the transcription s
e or Dragon Medical Netw
ternative dictation service.

teams are continuing to w
overy process and timing.

Everything is being done to re
and further updates will follow.

Mondelēz Intl @MDLZ
Follow

ebsite



WannaCry

- On Friday May 12, 2017, it infected more than 230,000 computers in over 150 countries
- Required no human interaction and spread over the internet
- Utilized an Exploit called EternalBlue
  - Microsoft released a patch March 14th, 2017
  - Released by hackers on April 14th, 2017
- Healthcare impact included:
  - Dharmais Hospital, Indonesia
  - Harapan Kita Hospital, Indonesia
  - U.K. National Health Services
- Multiple medical systems found vulnerable

NotPetya

- Began on June 27, 2017
- Targeted at Ukraine
- Spread like WannaCry but only on private networks
  - Can spread through vendor, business and VPN connections
- Healthcare impact included:
  - Heritage Valley Health System of Pittsburgh
  - Pharmaceutical company Merck & Co.
  - Software provider Nuance Communications

Using history to look forward

But wait, you just said all of this is a new concern!

- Attacker's motives stay the same
  - Money, fame, disruption, etc...
- Attacker's methods follow similar paths
  - They reuse what they know works
  - They use known exploits
  - Usually issues are patched prior to attacks

Sec_rity is incomplete without U!

- Watch for malicious or unsolicited emails
  - Take caution when opening attachments
  - Don't give out your password
- Patch!
  - Or ask about patching!
- Research past issues for your organization
- Tabletop incidents with your Security and IT teams
- Put pressures on vendors to uphold good security practices as well

Questions?

Resources

- https://www.privacyrights.org/data-breaches
- https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
- https://motherboard.vice.com/en_us/article/ezpzpe/the-spreading-epidemic-of-hospital-ransomware
- https://www.forbes.com/sites/thomasbrewster/2017/05/17/wannacry-ransomware-hit-real-medical-devices/
- http://money.cnn.com/2017/05/16/technology/hospitals-vulnerable-wannacry-ransomware/index.html
- http://www.healthcareitnews.com/news/nuance-knocked-offline-ransomware-attacking-europe
- http://www.darkreading.com/partner-perspectives/intel/healthcare-organizations-must-consider-the-financial-impact-of-ransomware-attacks/a/d-id/1325030