
Stories from the field

Sean Ebeling

LinkedIn - https://www.linkedin.com/in/seanebeling/

Professionally

- Worked in IT for over 30 years
- Held Architecture Positions in Healthcare and Pharma
- Leadership Degree from Villanova
- CISSP, Security Plus, Imprivata Certified Engineer

Personal

- Latch Key kid – don't touch the computer
- Wrote my first program in 1981 on a C64.
- I like to tinker with Raspberry PI, Arduino.
- Fun Stuff - Built my own arcade Cabinet, Brewed Beer, Mustang
- Wife, 2 kids, lots of Sports, Church

Social Engineering.
Can you go to California Monday?

- Why? I can't tell you.
- I am a Terrible Poker Player but…

  they gave me Domain Admin.
- How can we help?
  - Services - Assessment and Awareness training.

First VM in Azure!

- Senior level person wanted to be first.
- 2 NIC cards – one internal and one directly connected to the internet.
- The VM was hacked in less than 5 minutes.
- How can we help?
  - Monitor your cloud SAAS and IAAS environments for misconfigurations

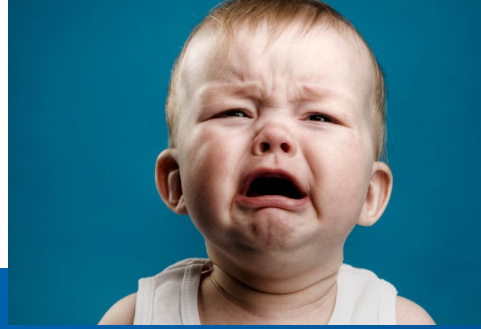
Entertainment Company
Exchange Hack

- Emails going out to customer and being used to steal credit card numbers.
- How did we help?
  - Services – Forensics
  - I joined the calls and offered some Powershell Expertise for collecting local account info.
  - Helped patch systems, change passwords etc.
  - How do we know they are gone? –MDR

Russian Compromise?
POC stops a major threat!

- County in the mid-Atlantic had legacy AV. We were showing them our product and doing a POC.
- Going well and rolled out to 100 systems. We so many alerts that I asked for one of our senior engineers to hop on the call and look. We found numerous dormant Viruses and even a connection back to a Russian server.
- How can we help?
    - EDR and MDR

Crying on Zoom



- Tried reaching out to a customer about security. He had some entitlements and couldn't get him to take our call.
- Called in the middle of an attack
- After some days of clean up, where he had multiple days of no sleep, he was crying.
- How can we help? Services, Pen Testing, Incident Response Retainer, Shoulder to Cry on!


DELL Technologies