Check Point
SOFTWARE TECHNOLOGIES LTD

# RANSOMWARE

## Survival guide


Anthony “AJ” Della Posta | Security Engineer

WELCOME TO THE FUTURE OF
CYBER SECURITY

POWERED BY CHECK POINT INFINITY

CLOUD • MOBILE • THREAT PREVENTION

# Chapters

- History and why?
- Bad Bugs
- How to prepare
- What to do when/if you are infected
- Post infection cleanup

# History, Why?

- Been around since 1989 – AIDS Trojan on Floppy disk
  - Targeted healthcare
- 2015 saw a massive surge in “Cryptoransomware”
  - Cheap to build
  - Easy to deploy
  - Guaranteed payment to the right targets
  - Fast and secured payment - Bitcoin
- In 2016 Ransomware alone will be a $1 Billion dollar industry globally
  - » NSA

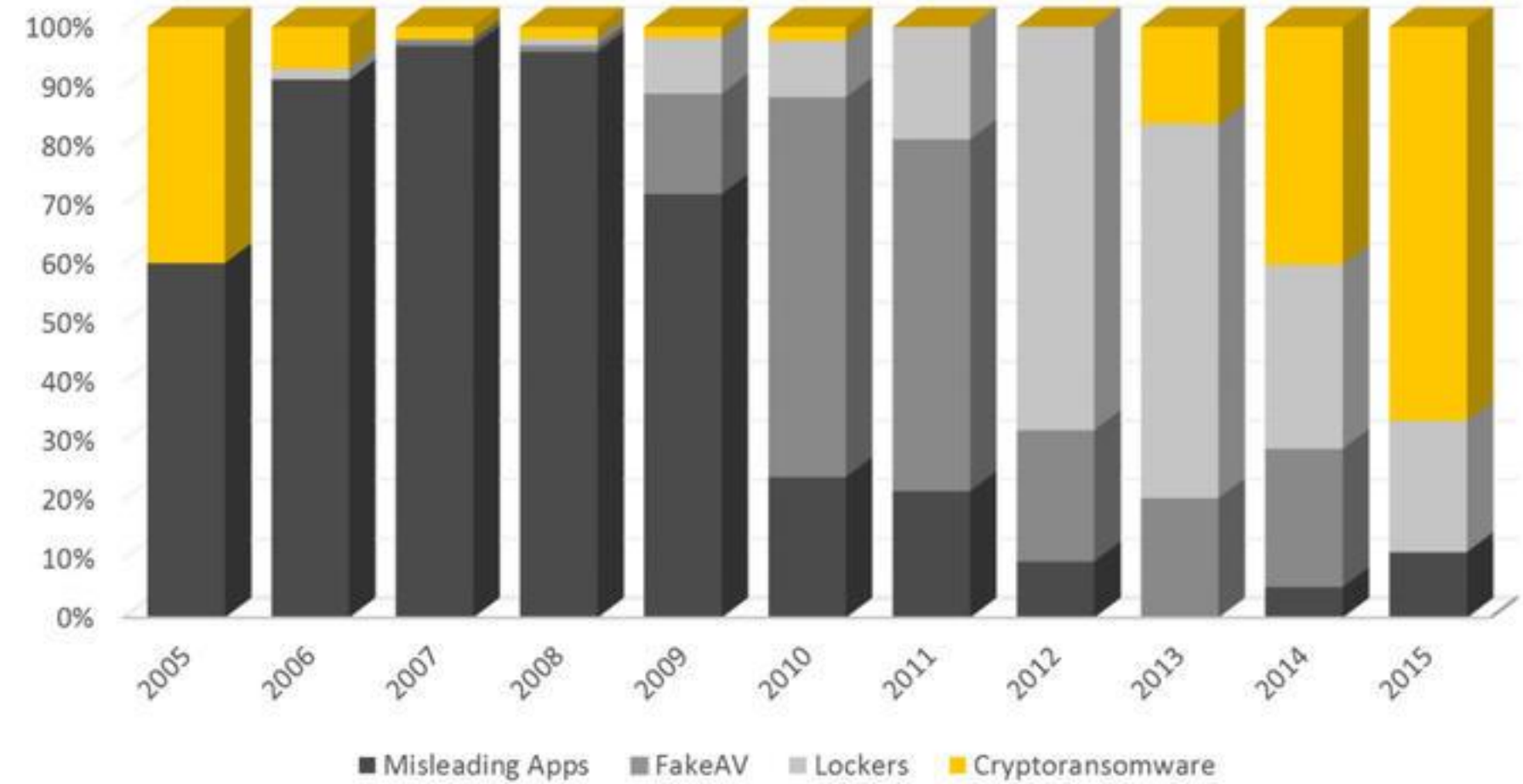



*Figure 4. Percentage of new families of misleading apps, fake AV, locker ransomware and crypto ransomware identified between 2005 and 2015*

# Bad Bugs

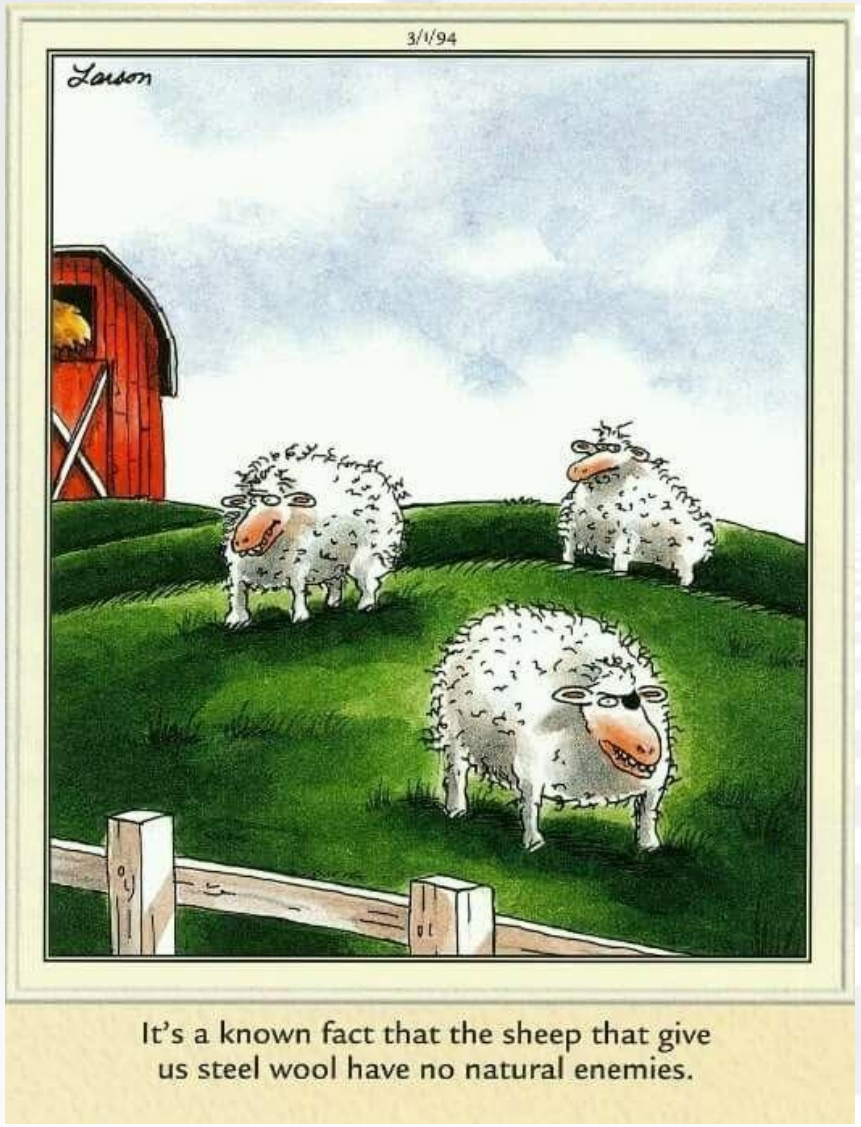
- Petya
  - Eastern Europe banking
- WannaCry
  - UK hospitals launched at lunch time
- Targets
  - Healthcare
  - Higher Education
  - Financials and Trading Companies
  - Small and Medium sized businesses

# Bad Bugs pt. 2

- Vectors of Attack
  - Email – phishing and attachments (macros)
  - Malicious URL's
  - Polymorphic malware that is sandbox aware
  - Mobile devices and IOT

# Prepare, Prepare, and Prepare

- Know the “fire drill” and share it with your team
- Basic safety precautions
  - Patch
  - Employee education
  - Remove EOL equipment
  - Backups – disconnect after use
    - Test backups
  - Isolate crown jewels (not just segmentation)
  - Patch (yes, its that important)



# Infection: Now what?

- Unplug and airplane mode immediately
- Don’t try and “google” a fix
- Don’t Pay
- Call the police – this is an extortion case
  - Call your IT partner
  - Call your security partner/vendor
    - Incident Response teams
  - Initiate Fire Drill plan
  - Wait
    - Law enforcement involvement, decryptions available

# After - Cleanup

- Review the tapes (logs)
  - How did it enter?
- Forensics report
- Report everything to law enforcement as well as your security partner
- Plug the holes
- Adjust “Fire plan”

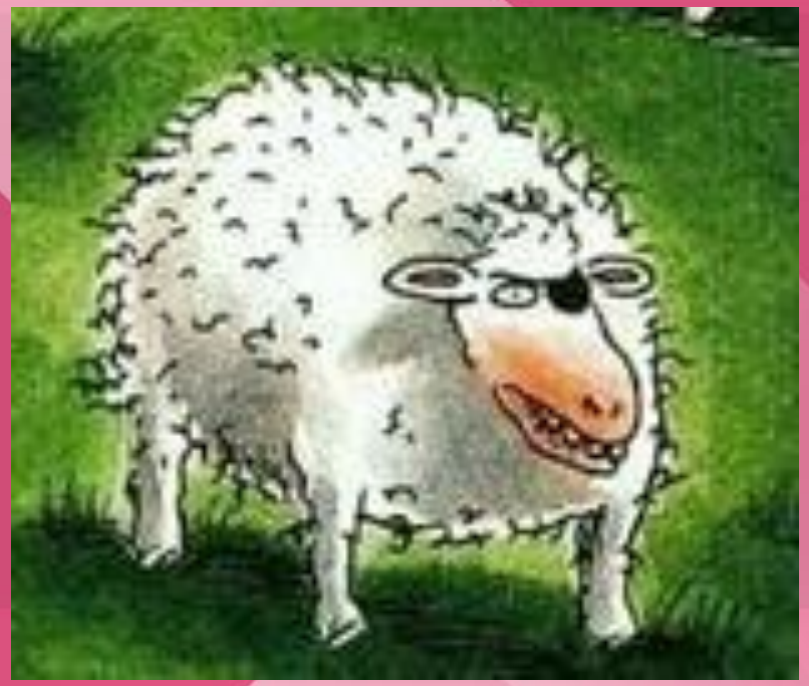
# Summary

- Prepare
- Don’t Pay
- Call

Check Point
SOFTWARE TECHNOLOGIES LTD

# THANK YOU

## Ransomware Survival Guide



Anthony “AJ” Della Posta | Security Engineer