CYBERSECURITY FRAUD: HOW TO ADDRESS RISK IN TODAY'S MARKETPLACE

Presented by:
Michael Cretaro, Consultant
ACC Technical Services

RISKS

- Improper IT maintenance/aging infrastructure
- Understanding cybersecurity vulnerabilities
- Lack of cybersecurity policy
- Confusing compliance with cybersecurity
- The human factor – people are the weakest link
- BYOD & the cloud
- Resource constraints
- Inadequate or non-existent business continuity & incident response plans
- Corporate inflexibility
- Accountability

@cc Technical Services

RANSOMWARE

LARGEST CURRENT THREAT

@cc Technical Services

WHAT IS RANSOMWARE?

"**Ransomware** is a type of malicious software from cryptovirology that blocks access to the victim's data or threatens to publish it until a ransom is paid."

-Wikipedia

A giant pain in the keister!

-Mike Cretaro

@cc Technical Services

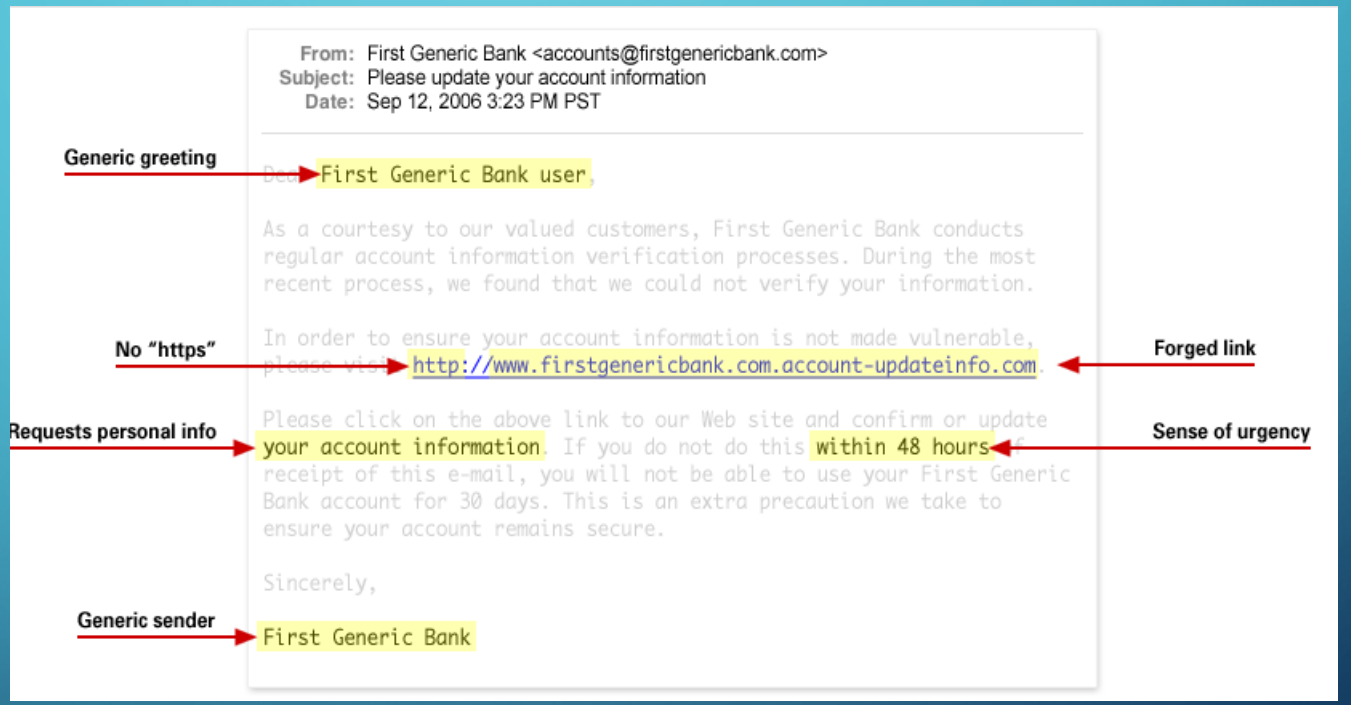
HOW DO WE GET RANSOMWARE?

- Email
- Unpatched software
- Thumb drives
- Websites
- Viruses
- Rerouted internet traffic
- SMS (text messaging)

Technical Services

HOW DO WE GET RANSOMWARE?

- Email



@cc Technical Services

HOW DO WE GET RANSOMWARE?

- Unpatched software
  - IOT – the Internet Of Things

@cc
Technical Services

HOW DO WE GET RANSOMWARE?

- Thumb drives

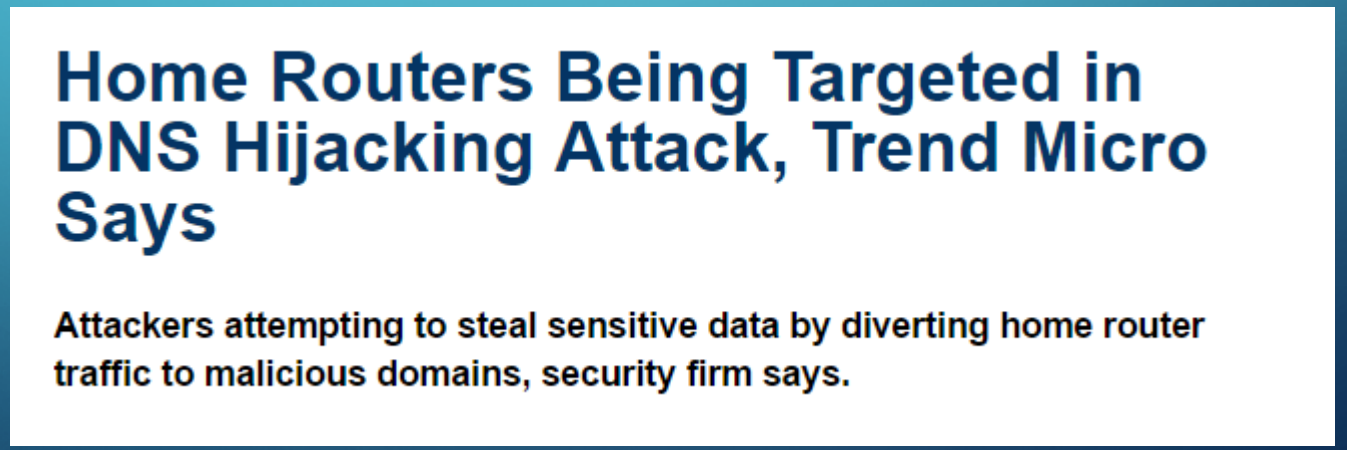
@cc
Technical Services

HOW DO WE GET RANSOMWARE?

- Websites
- Rerouted internet traffic

Major sites including New York Times and BBC hit by 'ransomware' malvertising

Adverts hijacked by malicious campaign that demands payment in bitcoin to unlock user computers



Home Routers Being Targeted in DNS Hijacking Attack, Trend Micro Says

Attackers attempting to steal sensitive data by diverting home router traffic to malicious domains, security firm says.

@cc Technical Services

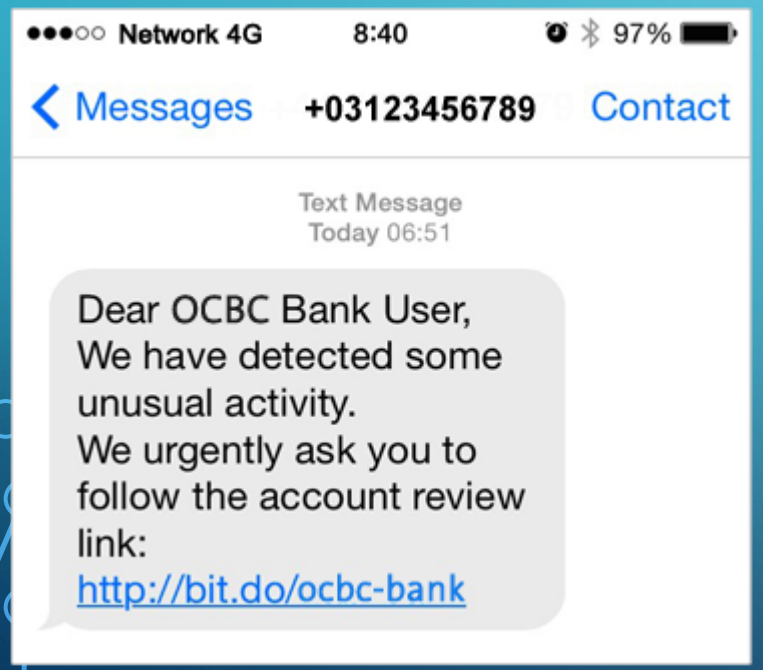
HOW DO WE GET RANSOMWARE?

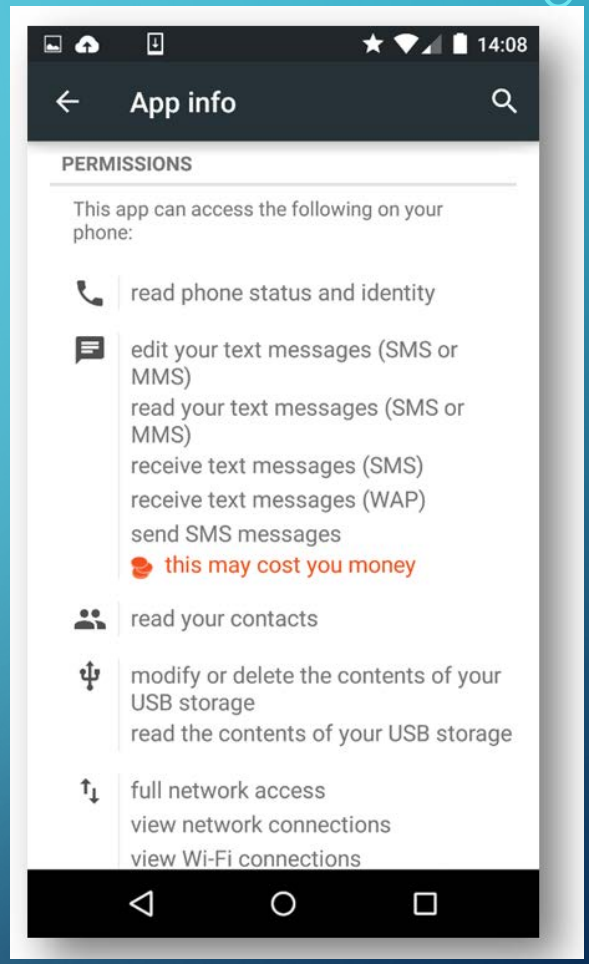
- Viruses

@cc
Technical Services

HOW DO WE GET RANSOMWARE?

- SMS (text messaging)





@cc Technical Services

Stolen credit card numbers worth a few dollars

TARGETS

- People are the #1 target
- Unpatched software
- Companies with valuable data
  - PII – Personally Identifiable Information
  - PHI – Protected Health Information
  - PCI – Payment Card Industry (credit card data)
  - Anyone with money

Stolen health records worth $350-$500 each

Technical Services

WHAT DOES IT DO?

- From the infected machine, it accesses every file it can
- Encrypts the data with strong encryption keys
- Exfiltrates the data for possible use later
- Deletes backups if accessible
- Notifies the user of the “ransom”
- Installs backdoors for possible later “re-infection”

HOW DO WE RECOVER?

- Should we pay the ransom?
  - There is no guarantee they will decrypt your files
  - Strong possibility they've stolen the data even if you pay
  - If you have good backups, then restore from backup
- Erase all affected systems and start over
  - Servers – if this was the point of infection – wipe and reload – can be time consuming
  - Workstations – erase and apply standard image – reinstall necessary applications
  - Share drives – delete share and restore from backups

@cc Technical Services

Security Is Uncomfortable

HOW DO WE PROTECT?

- Cybersecurity policy – including incident response
- Employee training
- Anti-virus & anti-malware software (only the start)
- DNS monitoring
- Backups: onsite and offsite
- Strong password policies
- Principle of Least Privilege
- LEM/SIEM – threat monitoring
- Cybersecurity insurance
- Pen test

@cc Technical Services

QUESTIONS?

Technical Services

CONTACT:

Michael Cretaro

Office: 315-484-4500

Cell: 315-952-6473

Email: mcretaro@acctek.com

@cc Technical Services