Simple Steps to More Security

Presenter:
C. Thomas (Space Rogue) Global Strategy Lead, X-Force Red
C. Thomas (Space Rogue)

- L0pht Heavy Industries
  - Whacked Mac Archives
  - Hacker News Network
  - CyberSquirrel 1
- Testified to Congress "Weak Computer Security in Government"
- Defcon, Blackhat, SOURCE, HOPE, BSidesLV
- MTV, ABC News, CNBC, CNN

X-Force Red Global Strategy Lead

c.thomas@ibm.com @spacerog
C. Thomas (Space Rogue)
C. Thomas (Space Rogue)

- Do Not Believe Anything I Say
- Everything Presented Here (or anywhere) is Biased
- Do Your Own Research

X-Force Red Global Strategy Lead

c.thomas@ibm.com  @spacerog
• Passwords
• Phishing
• Encryption
• Vulnerability Management (or Patching)
• Ransomware
• Have a Plan
• Even More You Can Do
Passwords

- Password Managers
Passwords

- Password Managers
Passwords

• Current NIST Guidance on Passwords
  □ Should be easy to remember but hard to guess
  □ Special characters no longer required
  □ 8 to 64 characters, passphrases preferred
  □ Never expire
  □ Copy and Paste password fields
Phishing

- Training
  - Needs to be continuous
  - Criminals are always evolving
  - Everyone makes mistakes
  - People are paid to click links
Encryption

- STARTTLS, DKIM, and S/MIME
- WPA2 (or WPA + TKIP/AES) for wireless
- No More http://
Vulnerability Management

X-FORCE RED VULNERABILITY DATABASE VULNERABILITIES PER YEAR

Year | Vulnerabilities
--- | ---
2008 | 7694
2009 | 6775
2010 | 8774
2011 | 7244
2012 | 8338
2013 | 8498
2014 | 9541
2015 | 9606
2016 | 10918
2017 | 16054
2018 | 16560
Vulnerability Management

- Vulnerabilities are infinite
- You will never patch them all
- Prioritizing
Ransomware

• Everyone is a target
Ransomware

- Everyone is a target
- Backups
  - Local and offsite
  - Daily snapshots
  - Test restores
Ransomware

- Everyone is a target
- Backups
  - Local and offsite
  - Daily snapshots
  - Test restores
- Restrict local Admin accounts
Have a Plan

- Who ya gonna call?

- “Everyone has a plan until they get punched in the mouth.”
Even more you can do

• Application whitelisting
• Clean out old user accounts
• Keep a tight reign on Admin accounts
• No local admin
• User education
• Authentication for processes
• MFA all the things
• Testing
Questions?

Presenter:
C. Thomas (Space Rogue) Global Strategy Lead, X-Force Red
THANK YOU

FOLLOW US ON:
- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

© Copyright IBM Corporation 2019. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represents only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or released or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.