Flash Memory Summit

PANEL 104-A

RansomWare
What It Is and What Role Does Flash Play ?

Organizer: Rich Fetik, Data Confidential

Chairperson: Mike McKean, Encore Semi, Inc.

Tue Aug 8th 4:55p – 6:00p

PANELISTS

Rich Fetik, CEO/CTO, Data Confidential

Devesh Ahuja, Security Consultant, Cipher Solutions

Prof. Hiroshi Watanabe, PhD, National Chiao Tung University (Taiwan)

Monty Forehand, Product Safety Officer, Seagate

Bob Thibadeau, CEO Bright Plaza Inc., Drive Trust Alliance

Flash Memory Summit

RansomWare : America’s Biggest cyber threat

Cipher Solutions inc.

CIPHER SOLUTIONS INC.
DATA SECURITY IS OUR PASSION

What is ransomware and what types exist?

- Ransomware – malware that demands payment for ‘a service’ (safe return of data or user access to a device, such as PC or USB)
- 3 Types of Ransomware: Scareware, Lockers and Crypto-ransomware
  - a). Scareware – demand for payment is made based on threat of future action using scare tactics
  - b). Lockers – promise of regaining access to user’s system or USB drive if met with demand for payment
  - c). Crypto-ransomware – after encrypting user’s files, crypto ransomware offers to sell the victim the decryption key for a fee

Examples of ransomware

- Cerber – spread via Windows Script Files (WSFs) inside double zipped attachments in 2016
- CryptoLocker – considered the ‘original’ ransonware which spawned other variants
- CryptoWall – randomizes filenames and encrypts documents found on the machine
- CTB-Locker – does not need to connect to a command and control server to encrypt files
- CryptXXX – provides payment instructions accessible via the TOR network
- WannaCry/WannaCryptor – spread by using exploits such as EternalBlue to attack unpatched vulnerabilities in the Windows OS SMB protocol. When WannaCry payload is executed, it encrypts files and demands $300 ransom

Flash Memory Summit

Ways to protect yourself from ransomware:

1. Keep your software updates current
2. Backup your data
   - Test your backups frequently
3. Have a good antivirus and keep it up to date
4. Avoid opening unsolicited email attachments and embedded links.
   - Train users to watch-out for click-jacking
   - Spoofed websites hidden behind some buttons user would often click e.g. close an ad or “win a free iPad”

Flash Memory Summit

Two notes on ransomware and Flash

Blockchained Storage Devices

Hiroshi Watanabe

Note-1: Infection Monitoring

- Infection of ransomware is data transaction between storage devices.
  - Monitoring data transaction as possible and save transaction record with no falsification.
  - Blockchain has a potential to satisfy this.

Note-2: Timestamp manipulation

- What will happen if ransomware will manipulate timestamp?
  - Hard to recover data in your storage device.
  - Blockchain and integrated batteryless timer may be candidates.

Trusting The Things

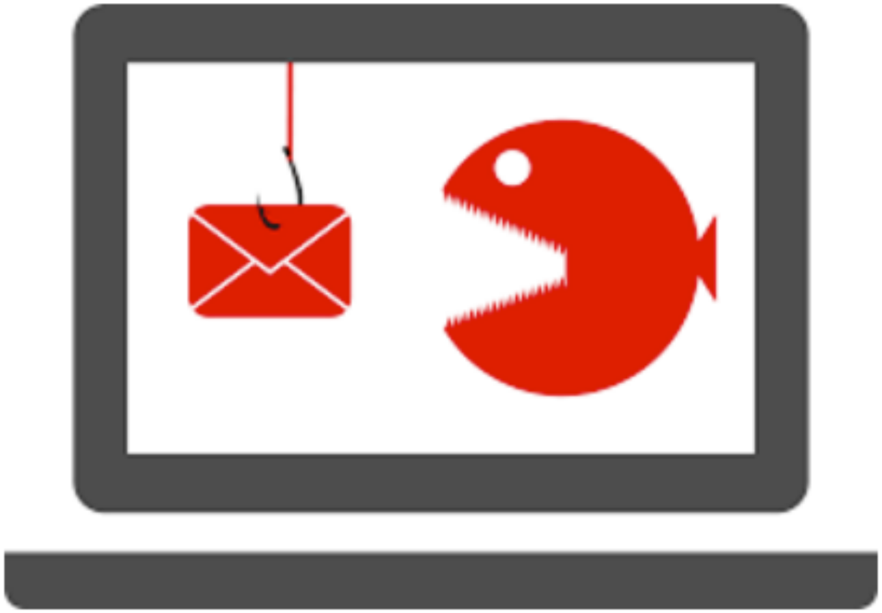
Ransomware Panel Session 104-A

Monty A. Forehand

Product Security Officer

Seagate Technology

1 in 10



34%

64%

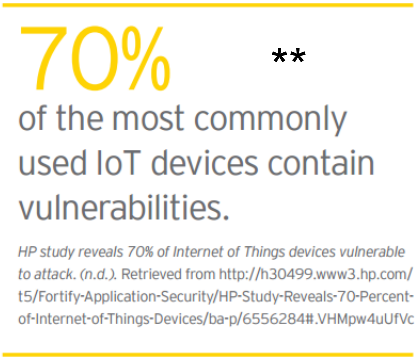
https://www.symantec.com/security-center/threat-report

47%

https://danielmiessler.com/study/red-blue-purple-teams/#gs.=3iGzD4

+

http://www.seagate.com/consumer/backup/backup-plus/



70% **

of the most commonly used IoT devices contain vulnerabilities.

HP study reveals 70% of Internet of Things devices vulnerable to attack. (n.d.). Retrieved from http://h30499.www3.hp.com/t5/Fortify-Application-Security/HP-Study-Reveals-70-Percent-of-Internet-of-Things-Devices/ba-p/6556284#.VHMpw4uUfVc

** Ernst & Young: Cybersecurity and the Internet of Things

Trusted

Thank You!

Visit Seagate Booth #505

Learn about Seagate's portfolio of SSDs, flash solutions and system level products for every segment.

www.seagate.com/Nytro