Security in the News
May 2017

It’s enough to make you cry!

Stuart Schwartz

Runner Ups

- IBM ships malware-infected USB drives
  - Any QC going on?
- Flaw allows hackers to reset password in WP 4.7.4
  - Notified July 2016
- Microsoft Edge was leaking passwords and cookies
  - So re-writing a browser is not bug free??
- Android "screen hijack” vulnerable until O
  - Seriously? Clickjacking gone mobile??

Yet More

- Microsoft Defender – Remote Code Execution
  - Google Project Zero rides again
  - Can be triggered by scanning an email (and others)
  - Very fast patching turnaround!
- Intel Active Management Technology (AMT)
  - Zero length password works
  - BIOS update needed
- One Minus
  - All OnePlus Devices Vulnerable to Remote Attacks
  - 4 unpatched vulnerabilities allows Man-in-the-Middle

OMG More??

- HP ships audio driver with a keylogger
  - Conexant driver v1.0.0.46 and earlier
  - Stores all activity in C:\users\public\MicTray.log
  - After reboot overwrites file
- Google Docs Phishing attack
  - Is this 1999?
  - Google blocked it quickly

Some Good News

- U.S. Supreme Court rules against Patent Trolls
  - 8 – 0 vote
    - Sends a strong message
  - No more “shopping” for friendly courts
  - 40 percent of all patent lawsuits filed in East Texas
    - 90 percent are brought by "patent trolls”
- Patent Troll
  - Company that buys one or more patents in order to force other companies pay by licensing or litigation
  - The troll does not use the patent directly

Want to Cry?

- WannaCry
  - Self spreading ransomware
  - NSA exploit EternalBlue leaked by Shadow Brokers
  - Affected Europe more than the US
    - Hospitals, telecommunications and utilities
  - Affects Windows 7 mostly, some XP
  - Patches also included EOL versions
    - XP and Vista!
- WannaCry kill switch (multiple sinkhole domains)
  - Researcher – ‘MalwareTech’ stopped for $11
- Prepare for the next attack!

Thank You!

Stu Schwartz
OWASP LA