Security Now! #510 - 06-02-15

Q&A #213

This week on Security Now!

- Crashing (your friends') iPhones,
- A worrisome Mac firmware problem.
- Microsoft annoying and/or frightening users with unsolicited "Win10 upgrade" offers,
- Google's Vault and Soli projects,
- Super-capacitor news,
- A bunch of Media Miscellany,
- The worlds first live demo of SQRL,
- And a Q&A with our listeners and viewers!

Microsoft frightens and confuses Windows users with unsolicited offers to reserve their free upgrade to Windows 10. Many assume they're been infected with malware!

Security News

iMessage Crash

- https://www.reddit.com/r/explainlikeimfive/comments/37edde/eli5_how_that_text_you_can_send_to_friends_turns/
- iOS 7 (iPhone 4, not 's') is safe. (iOS v7.1.2)
- Viewing in either the notification or preview (not conversation) mode causes the crash.
- "CopyFromStorage" API in the CoreText module
  - https://ghostbin.com/paste/zws9m

Crashing Macs,

- https://reverse.put.as/2015/05/29/the-empire-strikes-back-apple-how-your-mac-firmware-security-is-completely-broken/
- After a suspend-resume cycle, older Macs appear to be quite vulnerable to have their EFI Bios code overwritten by a malicious userland application.
- This allows for deep rootkitting since this code runs before the OS.
- Tested against a MacBook Pro Retina, a MacBook Pro 8.2, and a MacBook Air, all running latest EFI firmware available. All are vulnerable.
- It appears that latest MacBook models are NOT vulnerable, but the author/discoverer could not be 100% certain.
- He suspects, with little proof, that the bug in suspend-resume handling was silently fixed by Apple but that all mid/late 2014 machines, and newer, are not vulnerable.
- But all older machines, for which Apple is no longer providing firmware updates, appear to be.
- Mitigation:
    - Don't use Sleep, only use Shutdown.
    - Run as Admin (non-root) account.
    - Get updated firmware from Apple.
    - Get a newer Mac.

All roads lead to Windows 10...

- http://windows.microsoft.com/en-us/windows/preview-download
- http://www.idigitaltimes.com/windows-10-update-icon-real-how-can-i-remove-it-cautious-users-worry-theyve-been-445716
- "Get Windows 10" free upgrade "reservation."
- How to remove?
    - Remove the ‘Get Windows 10’ icon the same way you would any other update:
    - Go to Control Panel -> Programs and Features -> Uninstall an update -> look for "KB3035583" and “KB2952664” and uninstall them.
    - Reboot and the icon should be gone.
    - When W10 itself comes, you'll have to check in Windows Update manually.

Project Vault - Google I/O ATAP - Advanced Technologies and Products

- HSM - Hardware Security Module.
- High speed bulk crypto: encryption and decryption.
- Supports secure streaming operations.
- Just as Yubico used USB keyboard emulation, this it's able to use any OS's existing drivers.
- Vault creates a virtual file system with a single virtual read-only and a write-only file so that, once again, any OS's existing drivers can be reused.

Project Soli - Google I/O ATAP - Advanced Technologies and Products

- http://bit.ly/sn-510c
- https://www.youtube.com/watch?v=0QNiZfSsPc0
- Super high-resolution, super high frame rate, 60Ghz radar.
- 60Ghz wavelength is 5mm -- 1/5th inch.
- 0.05m to 5m range with 180 degree field of view.
- Signal in 60GHz band are strictly range-limited due to absorption by Oxygen molecules. This limits the operational range to short distances.
- Japanese vehicular radar operates in the 60.5 Ghz band.

SuperCapacitor Watch:

- http://www.marketwatch.com/story/sunvault-energy-and-edison-power-company-create-massive-10000-farad-graphene-supercapacitor-2015-05-06
- http://www.sunvaultenergy.com/
- 10,000 Farad capacitors... but no where is there a statement of the breakdown voltage.
- Petrochemical - gas. Does not combust too easily, non-renewable, but fast to refill.
- Electrochemical - batteries. Limited lifetime, noxious chemistries, slow to refill.
- Electromechanical - flywheel. Extremely dangerous in a crash. Renewable, can be fast to spin up.
- Electrostatic - supercapacitor. A bit scary in a crash, renewable, can be fast to refill.

Media Miscellany:

The backwards bicycle (via "1roge" @1roge)

- Backward Brain Bike thought of you youtu.be/MFzDaBzBlL0
- http://bit.ly/sn-510a

Mr. Robot on USA Networks (IMDB 9.4/10 from 4,800 reviewers.)

- Free: VUDU, YouTube,
- http://bit.ly/sn-510b
- http://www.imdb.com/title/tt4158110/

Project Almanac

- High school (unsteady cam) kids build a time machine... what could go wrong??

Halt & Catch Fire,

- Season 2 has resumed

"The Strain" on FX.

- 1st season, July 13th, 13 episodes.
- Resumes July 12th... another 13 episodes.

Orphan Black

- Season 3 went off the rails for me. (Like when Battlestar Galactica lost it.)

Blockwick (Blockwick 101 is free)

SQRL's first-ever live demo...

SpinRite:

Date: Mon, 18 May 2015 17:45:40 -0700
From: Kyle Schmidt, Cheyenne Wyoming

Just another SpinRite success story to share:

I have a VIAO Win7 Pro laptop that I HAD to purchase while travelling on business through Seoul Inchon airport at a duty free shop (laptop that I was travelling with crashed). About a month ago, I was carrying same and dropped it while it was on, and even though it has a "shock protected" HDD, the results were predictable.

After numerous unsuccessful attempts at Windows repair, etc, I remembered SpinRite from GRC and even though it took almost a day and a half to totally rejuvenate the very troubled HDD, lo and behold, it once again boots up and is usable.

There were sectors that are still unrecoverable, but SpinRite was able to "raise it from the dead"! Thanks for continuing to offer the utility, I can personally attest to the fact that IT WORKS AS PROMISED!

Regards,

Kyle Schmidt
Cheyenne Wyoming