Security Now! #522 - 08-25-15

Q&A #217

This week on Security Now!

- Lenovo BIOS behavior retraction and update
- Ransomware file encryptor appears on Github
- Many changes coming to Firefox
- Consequences of the growing intersection of life and the Internet.
- The best thing about Google's new Router.
- The need for physical security and Hillary's eMail server.
- Miscellany
- Feedback, thoughts and questions from our terrific listeners.

Security News:

Finally... things slow down!

- Matthew Green (@matthew_d_green) 7:41am · 25 Aug 2015 · Twitter for iPhone
- It's almost as though people blew all the interesting security results on BlackHat and Defcon, then took the rest of August off.

Lenovo, having been caught (again) removes its funky BIOS-push technology

- http://news.lenovo.com/article_display.cfm?article_id=2013
- LSE = Lenovo Service Engine.
- "Lenovo's use of LSE was not consistent with [Microsoft's] guidelines. As a result, LSE is no longer being installed on Lenovo systems. It is strongly recommended that customers update their systems with the new BIOS firmware which disables and or removes this feature".
- https://support.lenovo.com/us/en/product_security/lse_bios_desktop
- https://support.lenovo.com/us/en/product_security/lse_bios_notebook
- http://bit.ly/sn-522
    - List of affected Lenovo Products:...

Ransomware encrypter goes to Github:

- https://github.com/utkusen/hidden-tear
- Description:
    - It's a ransomware-like file crypter sample which can be modified for specific purposes.

- Features:
  - Uses AES algorithm to encrypt files.
  - Sends encryption key to a server.
  - Encrypted files can be decrypt in decrypter program with encryption key.
  - Creates a text file in Desktop with given message.
  - Small file size (12 KB)
  - Doesn't detected to antivirus programs (15/08/2015) http://nodistribute.com/result/6a4jDwi83Fzt
  - Target file extensions can be change. Default list:
    - var validExtensions = new[]{".txt", ".doc", ".docx", ".xls", ".xlsx", ".ppt", ".pptx", ".odt", ".jpg", ".png", ".csv", ".sql", ".mdb", ".sln", ".php", ".asp", ".aspx", ".html", ".xml", ".psd"};
- Legal Warning
  - While this may be helpful for some, there are significant risks. hidden tear may be used only for Educational Purposes. Do not use it as a ransomware! You could go to jail on obstruction of justice charges just for running hidden tear, even though you are innocent.

Firefox Extension Signing

- https://wiki.mozilla.org/Addons/Extension_Signing
- https://addons.mozilla.org/en-US/firefox/
- Essentially… proactive rather than reactive - enhanced upfront curation.
- Status & Plan:
  - Firefox 40: Firefox warns about signatures but doesn't enforce them.
  - Firefox 41: Firefox will have a preference that allows signature enforcement to be disabled (xpinstall.signatures.required in about:config). --> Currently "false" in v40
  - Firefox 42: Release and Beta versions of Firefox will not allow unsigned extensions to be installed, with no override.
- The Case for Extension Signing
  - https://blog.mozilla.org/addons/2015/04/15/the-case-for-extension-signing/
  - Moving toward a more curated model to minimize malicious add-ons.
- All main browser extensions have recently been getting themselves signed.

Mozilla moving toward Chrome's Extensions API

- https://blog.mozilla.org/addons/2015/08/21/the-future-of-developing-firefox-add-ons/
- Firefox Extension API will be migrating to "WebExtension" in the future.
- "WebExtensions" - Largely compatible with the model used by Chrome & Opera (and Edge)

Consequences of the growing intersection of life and Internet technology

- Ashley Madison
- Google election skewing
- http://www.politico.com/magazine/story/2015/08/how-google-could-rig-the-2016-election-121548.html
- PNAS - Proceedings of the National Academy of Sciences

- The search engine manipulation effect (SEME) and its possible impact on the outcomes of elections.
- We present evidence from five experiments in two countries suggesting the power and robustness of the search engine manipulation effect (SEME). Specifically, we show that (i) biased search rankings can shift the voting preferences of undecided voters by 20% or more, (ii) the shift can be much higher in some demographic groups, and (iii) such rankings can be masked so that people show no awareness of the manipulation. Knowing the proportion of undecided voters in a population who have Internet access, along with the proportion of those voters who can be influenced using SEME, allows one to calculate the win margin below which SEME might be able to determine an election outcome.
- Election 2016 in Google searches
- https://www.google.com/trends/story/c5c95ce9-6b74-4939-b112-57e405ef0109
- <quote> According to Google Trends, at this writing Donald Trump is currently trouncing all other candidates in search activity in 47 of 50 states. Could this activity push him higher in search rankings, and could higher rankings in turn bring him more support? Most definitely—depending, that is, on how Google employees choose to adjust numeric weightings in the search algorithm. Google acknowledges adjusting the algorithm 600 times a year, but the process is secret, so what effect Mr. Trump's success will have on how he shows up in Google searches is presumably out of his hands.

Hillary eMail physical security / An apparent failure of due diligence.

- Headline: EXCLUSIVE: Hillary's email firm was run from a loft apartment with its servers in the BATHROOM, raising new questions over security of sensitive messages she held.
- According to former employees, "The servers were in a closet off the bathroom."
- Quote: 'I don't know how they run their operation now, but we literally had our server racks in the bathroom.'
- Level3: Coded inductive badge, Right hand biometrics, PIN, Combination lock... conspicuous cameras, and onsight 24/7 human security patrol.

Google Router

- Best feature from the FAQ: OnHub also automatically updates without interrupting your Wi-Fi connection so you'll always have the latest features and security upgrades.
- For my own needs, I need a FreeBSD UNIX doing my routing… but if its WiFi is really strong and it can be use as an access point, then definitely.

Miscellany

- Humans & Mr.Robot

SpinRite:

- What does it do???
- Security Now keeps growing, so we have many new listeners.