Security Now! #561 - 05-24-16

Q&A #234

This week on Security Now!

- A surprising end to the Teslacrypt file encrypting malware
- Google's plan to continue squeezing Flash off the web
- Anyone want 117 million (old) LinkedIn eMail addresses and passwords? They're for sale.
- News of the technology underlying Google's new Allo messaging system
- Cory Doctorow is fighting the good fight for data freedom
- A bit of miscellany and... questions and comments from our terrific listeners!

Security News

TeslaCrypt shuts down and Releases Master Decryption Key

http://www.bleepingcomputer.com/news/security/teslacrypt-shuts-down-and-releases-master-decryption-key/

- In a surprising end to TeslaCrypt, the developers shut down their ransomware and released the master decryption key. Over the past few weeks, an analyst for ESET had noticed that the developers of TeslaCrypt had been slowly closing their doors, while their previous distributors have been switching over to distributing the CryptXXX ransomware.
- Apparently thinking "what the hell", the ESET security researcher posted to TeslaCrypt's support chat, asking if they would consider releasing the master decryption key. They did.
- Now, the TeslaCrypt decrypting utility "TeslaDecoder" is at v1.0 and can decrypt v3 and v4 TeslaCrypt encrypted files.
- ESET also has a command-line decryptor http://www.welivesecurity.com/2016/05/18/eset-releases-decryptor-recent-variants-teslacrypt-ransomware/

Google's Chrome browser continues to squeeze Flash out

http://venturebeat.com/2016/05/15/google-targets-html5-default-for-chrome-instead-of-flash-in-q4-2016/

- Recap: Last September, Chrome 45 began pausing any FLASH content that was not "central" to the web page being displayed.
- Now, beginning in Q4 2016, Google intends to focus on "central content" such as games

and videos.

- Google calls this new initiative "**HTML5 by Default**"
- Flash Player will continue to be bundled with Chrome, however its presence will not be advertised by default. (Not listed in navigator.plugins[] or navigator.mimeTypes[])
- If a site offers an HTML5 experience, that becomes the default experience.
- When a user encounters a site that needs Flash Player, a prompt will appear at the top of the page, giving the user the option of allowing it for a site.
- If the user accepts, Chrome will advertise the presence of Flash Player, and refresh the page.
- Chrome will honor the user's setting for that domain on subsequent visits.
- To avoid over-prompting users, Google will initially ship with a whitelist of the then top 10 sites (based on aggregate usage). This whitelist will expire after one year.
- Some sites, like Pandora.com, direct users to download Flash Player, when they don't see it advertised. Once the user clicks on the download link (i.e. get.adobe.com/flashplayer) Google will intercept the request, cancel the navigation, and instead present an "Allow Flash Player …" infobar, with behavior consistent to the previous flow.
- Enterprises will be given a policy setting to "Always run FLASH content."
- Under Content Settings, users may opt to "Always run FLASH content" and manage individual site preferences.
    - Always run Flash content
    - Allow Sites to ask to run Flash
    - Let me choose whether for a site
    - Never run Flash content

117 million Linked-In eMail addresses and passwords from a 2012 hack posted online

- To recap: Four years ago, back in 2012, hackers obtained ~6.5 million encrypted passwords, and posted them onto a Russian hacker forum.
- Because the passwords were stored as unsalted SHA-1 hashes, hundreds of thousands were quickly cracked.
- Today, a hacker going by the moniker "Peace" is offering data for 167 million LinkedIn accounts -- stolen from the same dataset -- 117 million of which contain both eMail address and password, and thus also only hashed with SHA1 with no salt added.
- "Peace" is asking about $2200 USD payable in Bitcoin.
- 90 percent of the passwords were cracked within three days (72 hours) and used to log into their LinkedIn account... since their owners hadn't changed their password after the initial breach.
- The Register.co.uk snarkily reports that LinkedIn users haven't learned any lessons about proper passwords.

Allo - Won't have encryption enabled by default?

- Why? Because then Google would be unable to see into the chat to add its value.
- For Google to add dinners with friends to calendars or suggest replies (an Allo feature), it must be able to see into the chat — which it can't do if chats are end-to-end encrypted.
- So Allo offers users a choice: privacy and security, or entertainment and interactivity.
- TechCrunch, in covering this, suggests that most consumers will likely choose the latter, leaving security by the wayside.
- Is Allo's encryption any good? Oh yes. Those who choose to turn on Allo's encryption, dubbed "incognito mode," will be using Open Whisper Systems Signal Protocol. Nice.

Cory Doctorow: "Save Firefox!" / May 11th, 2016
https://www.eff.org/deeplinks/2016/04/save-firefox

Miscellany

Never10 uptake rate

- Never10: Now at 25,000 copies/day
- **Paul Thurrott: May 24th**
- "Upgradegate: Microsoft's Upgrade Deceptions Are Undermining Windows 10"
- https://www.thurrott.com/windows/windows-10/67367/upgradegate-microsofts-upgrade-deceptions-undermining-windows-10

- **Graham Cluley: May 24th**
- Microsoft has a dirty little Windows 10 upgrade trick up its sleeve.
  Clicking "X" won't stop your PC upgrading to Windows 10.
- https://www.grahamcluley.com/2016/05/microsoft-dirty-little-windows-10-upgrade-trick-sleeve/

- **Brad Chacos, senior editor at *PC World***, is one of those who considers this to be a "nasty" trick:
- "So after more than half a year of teaching people that the only way to say "no thanks" to Windows 10 is to exit the GWX application—and refusing to allow users to disable the pop-up in any obvious manner, so they *had* to press that **X** over and over again during those six months to the point that most people probably just click it without reading now - Microsoft just made it so that very behavior accepts the Windows 10 upgrade instead, rather than canceling it."

  "Deploying these dirty tricks only frustrates long-time Windows users who have very valid reasons to stick with operating systems they already know and love."

Seriphos and the HSF

- Seriphos
- Enerphos / T.E. Neesby

SpinRite

Curt M in Southern California

Subject: My personal experience with an old friend "SpinRite"
Date: 20 May 2016 20:22:33
:
Dear Steve,

In the 1970's, you would call the TV repairman to replace the tubes in your TV.

They were very expensive, and went out often. In the 1980's, computers were much the same.

Hard drives, though more reliable than floppy discs, for anyone who still remembers, that's not saying much.

As a young man in the 80s, I spent many an hour working in computer repair. The problems were many, from Compaq, and Mac-128K power supplies, to 30mb Seagate RLL drives - which was really just a 20MB drive with a different controller. Drives of that era were just not very reliable.

Over the course of my lifetime, I have repaired hundreds, if not thousands of hard drives.
You know how many times after all those years SpinRite failed me?

0, Zero, nada. Wow!

To me, SpinRite is the Rock of Gibraltar. I've always felt, that if you know SpinRite, you know the man behind it. I believe it was a labor of love, and it shows in the end product. And if you love what you do, then you understand in intimate detail the principles of what makes it all tick. It's clear that you do.

Thanks for giving the world a product they can truly trust. I can attest that with SpinRite, you can trust it like an old friend.

Respectfully, Curt M.