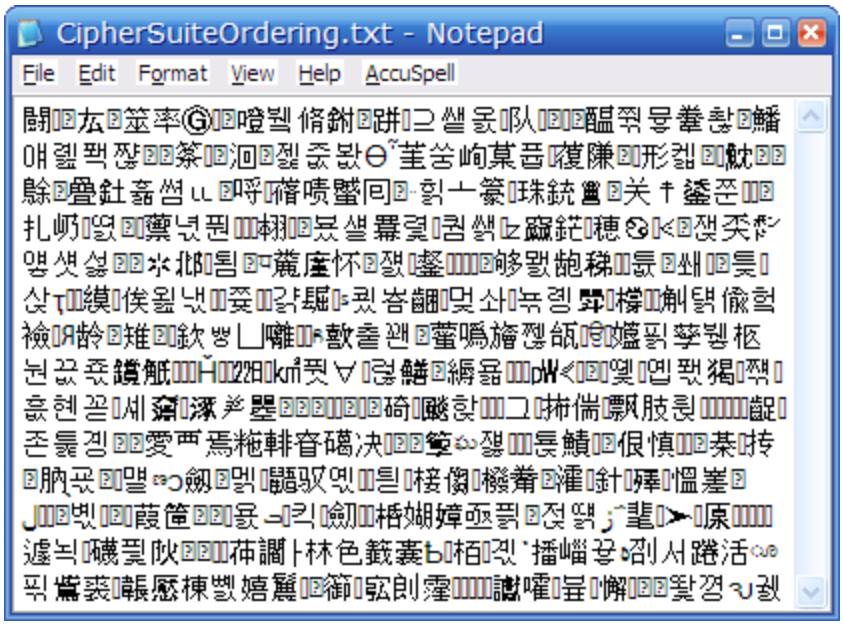
Security Now! #497 - 03-03-15

Hacking Vehicles

This week on Security Now!

- Another set of SoHo router backdoors.
- An interesting, but not yet perfect, web-based encryption service.
- Create an Internet service, have your life threatened.
- The evolution of DNS.
- The evolution of search.
- Miscellaneous goodies.
- This week's feature: Hacking Vehicles

Un-Authenticated Encryption



www.InstantCryptor.com

Security News

Another Router Backdoor Discovered

- International Conference on Cyber Security and Cyber Law 2015 (Feb 21)
- http://blog.ensolnepal.com/router_backdoor/
- Supervisor username and password were both "super"
- 200,000+ found, so likely around half a million total.
- Most appear to be off-brand.

Appears that router firmware was stolen.

- Digicom
  - DAPR 150RN
  - DAPR 300RN
- Alpha Network
  - AIP-W525H
  - AWAP806N
- Pro-Link
  - PRN3001
  - WNR1008
- Planet Networks
  - WNRT-300G
- TrendNet
  - TEW-638APB
  - TEW-639GR
  - TWE-736RE
- Realtek
  - RTL8181
  - RTL8186
  - RTL8186P
- Bless
  - Zio-3300N
  - Zio-4400N
  - Zio-3200N
  - Zio-3300N
- SmartGate
  - SG3300N
  - SG3100N
- Blue Link
  - BL-R30G

InstantCryptor

- https://instantcryptor.com/index.html
- Works with Firefox or Chrome
- Dropbox or Google Drive
- <documentation> “The password will be hashed with the SHA256 algorithm, the mode for encryption is 256 Bit Rijndael/AES (CBC mode). The file Blob will be read as an ArrayBuffer and fed into the encryption function. The result is then uploaded to the chosen cloud service. The uploaded files are displayed in the tool and decryption works accordingly. The code of the main JavaScript file is unminified and the interested developer can have a look at it, the main action happens in the last two functions at the end of the file.”
- Not using Authenticated Encryption.
  - This means that there's no assurance that a decrypted file has not been modified.
  - Naive users can be forgiven for thinking that an encrypted file cannot be meaningfully modified, but years of experience has taught us otherwise. That's why SSL & TLS always authenticate.

- Authentication should be applied to the encrypted data so that the first thing done before attempting to decrypt is to verify that the file that's about to be decrypted has not been modified from the original.

Create an Internet service, have your life threatened:

- ISIS supporters on Sunday called on jihadis around the world to kill Twitter employees because of the company's frequent blocking of their social media accounts.
- An online post (since removed) addressed to Twitter founder Jack Dorsey on "Just Paste It" reads: "Your virtual war on us will cause a real war on you." The post was shared by ISIS supporters.
- The post, whose authorship is unclear, was accompanied by a digitally altered image of Dorsey in the cross sights of a gun.

The evolution of Internet Top Level Domains (TLDs)

- Google just paid $25 million for the entire "*.app" top level domain. Why?
- Amazon paid $5M for *.buy and $2.2M for "*.spot"
- Dot Tech paid $6.7M for *.tech
- Amazon has appiled for 76 gTLDs and Google has applied for 101.
- Google also wants .blog, .cloud and .search.
- Two tidbits:
- .blog : ... our application for the .blog TLD describes a new way of automatically linking new second level domains to blogs on our Blogger platform – this approach eliminates the need for any technical configuration on the part of the user and thus makes the domain name more user friendly.
- .dev : Second-level domain names within the [.dev] proposed gTLD are intended for registration and use by Google only, and domain names under the new [.dev] gTLD will not be available to the general public for purchase, sale, or registration. As such, Google intends to apply for an exemption to the ICANN Registry Operator Code of Conduct as Google is intended to be the sole registrar and registrant.
- http://sealedabstract.com/rants/google-our-patron-saint-of-the-closed-web/

Google to rank sites by "truthfullness"

- "Knowledge-Based Trust" (KBT)
- "Estimating the Trustworthiness of Web Sources."
- <quote> "A source that has few false facts is considered to be trustworthy."
- http://arxiv.org/pdf/1502.03519v1.pdf
- The "Knowledge Vault"
- http://www.newscientist.com/article/mg22329832.700-googles-factchecking-bots-build-vast-knowledge-bank.html
- Knowledge Vault has pulled in 1.6 billion facts to date. Of these, 271 million are rated as "confident facts", to which Google's model ascribes a more than 90 per cent chance of being true. It does this by cross-referencing new facts with what it already knows.

Miscellany:

Spock and Roddenberry @ Comdex
- "ShieldsUp!"

Media:
- Citizen Four
- The Good Wife
- The Immitation Game
- ... The Americans
- ... Justified

Podcast Awards now open through March for voting.
- http://podcastawards.com/
- Vote for SN... vote often!

Cornell University researchers model the Zombie Outbreak
- http://mattbierbaum.github.io/zombies-usa/
- Best places to be? The Northern Rockies.
- http://www.vox.com/2015/3/3/8140945/zombie-apocalypse-science

SpinRite:

Francisco Gomez
Date: Tue, 24 Feb 2015 00:37:20 -0800
Subject: Oh my god. You guys are incredible/SpinRite

I could right a loooong email telling you how great you are. But after 12 hrs other people spent fighting and failing to get the data restored, you guys made me look like a hero in front of my wife. Her I.T. department said she had lost all of her data. But after using SpinRite and running check disk I was able to extract ALL of the data even when the HDD was encrypted.

You guys are geniuses

Sent from my iPhone

Hacking Vehicles