Security Now! #504 - 04-21-15

Great Firewalls & Cannons

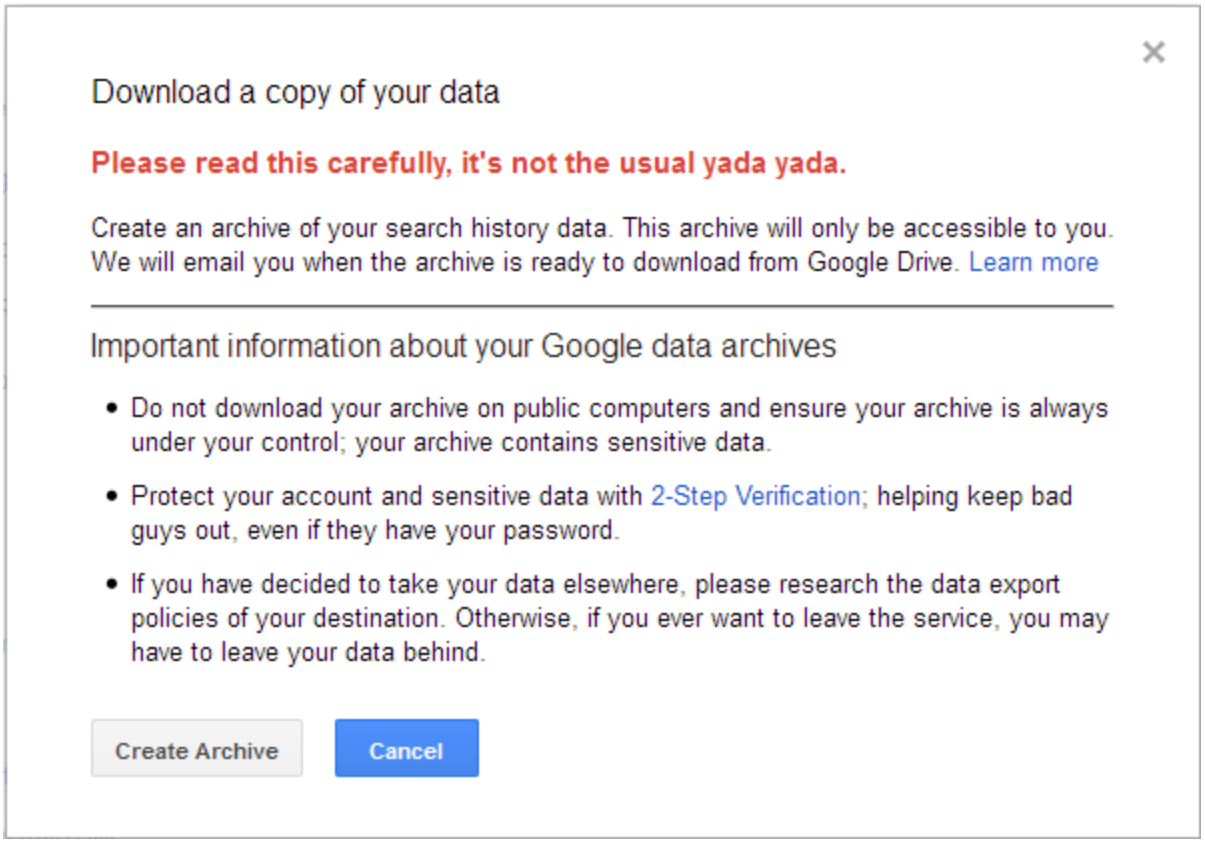
Before the show with Leo:

- Madmen - still great writing... but... huh?
- Why is game of thrones so riveting?
- Silicon Valley getting better and better.
- Halt and Catch Fire will be returning.

This week on Security Now!

- TrueCrypt audit follow up
- IIS under BSOD attack
- Google search history dump
- Chrome drops support for older plugins
- Popular iOS networking library had a bad problem.
- News of "Let's Encrypt"
- China's attempts to control the Internet.

Google offers download of user's entire search history...



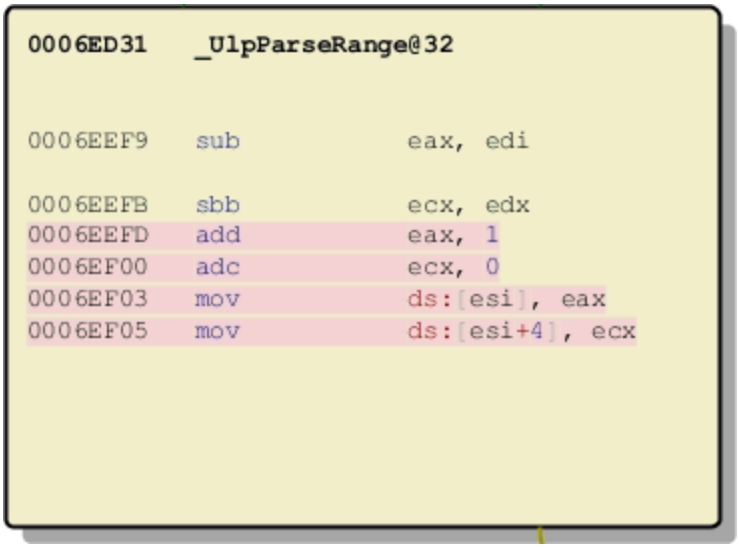
TrueCrypt Audit Follow Up:

An interesting note from "Tom Ritter" cryptographer and managerial lead of NCC:
https://threatpost.com/post-cryptanalysis-truecrypt-alternatives-step-forward/112033
<quote> Tom Ritter: "The audits of TrueCrypt get a lot of press because it's something flashy, but the development effort that went into TrueCrypt at the beginning are immense and incredible, and the developers don't get as much credit as they should for producing a disk and volume encryption project for multiple platforms and for maintaining it for a decade or more. There are successor projects and they are improving it in their own ways. I am excited to see those projects grow and thrive and last as long as TrueCrypt did. I still use TrueCrypt and want to see it supported in the future."

Security News

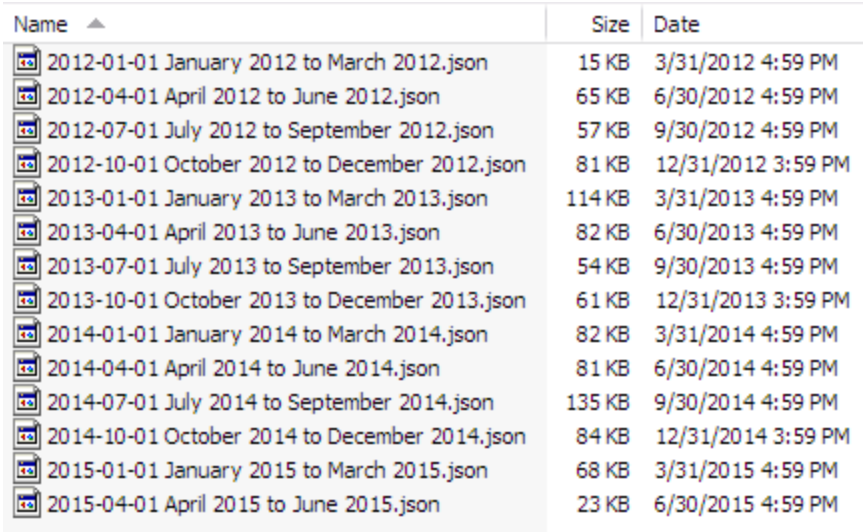
The bad bug in IIS (MS15-034)

- Affected: Windows 7, Windows Server 2008 R2, Windows 8 and 8.1, Windows Server 2012 and 2012 R2 Server Core installation option.
- Active attempts to crash IIS servers underway.
- Netcraft estimates an exposure of 70 Million IIS servers.
- HTTP.SYS
    - Microsoft saw an opportunity for performance improvement by moving a chunk of their IIS server into the kernel: Parsing just enough of an HTTP request to see whether it can be fulfilled from a cache of previous responses, which is also in the kernel.
    - This is not unlike moving video drivers into the kernel.
    - The trouble is, ANY MISTAKE in the code no longer crashes an operating system client process... now it takes the entire OS down.to A lowest-level driver which system library that implements the parsing of http requests and implements caching content in kernel memory."
- Range: bytes=2-18446744073709551615
- Reverse Engineering:
- http://blog.beyondtrust.com/the-delicate-art-of-remote-checks-a-glance-into-ms15-034



Obtain Your Google Search History

- http://googlesystem.blogspot.com/2015/04/export-google-search-history.html
- Steps:
  - Goto: https://history.google.com/history/
  - Acknowledge the dialog…
  - Wait for eMail archive to be prepared.
- "Takeout" folder appeared containing a ZIP file.



Name	Size	Date
2012-01-01 January 2012 to March 2012.json	15 KB	3/31/2012 4:59 PM
2012-04-01 April 2012 to June 2012.json	65 KB	6/30/2012 4:59 PM
2012-07-01 July 2012 to September 2012.json	57 KB	9/30/2012 4:59 PM
2012-10-01 October 2012 to December 2012.json	81 KB	12/31/2012 3:59 PM
2013-01-01 January 2013 to March 2013.json	114 KB	3/31/2013 4:59 PM
2013-04-01 April 2013 to June 2013.json	82 KB	6/30/2013 4:59 PM
2013-07-01 July 2013 to September 2013.json	54 KB	9/30/2013 4:59 PM
2013-10-01 October 2013 to December 2013.json	61 KB	12/31/2013 3:59 PM
2014-01-01 January 2014 to March 2014.json	82 KB	3/31/2014 4:59 PM
2014-04-01 April 2014 to June 2014.json	81 KB	6/30/2014 4:59 PM
2014-07-01 July 2014 to September 2014.json	135 KB	9/30/2014 4:59 PM
2014-10-01 October 2014 to December 2014.json	84 KB	12/31/2014 3:59 PM
2015-01-01 January 2015 to March 2015.json	68 KB	3/31/2015 4:59 PM
2015-04-01 April 2015 to June 2015.json	23 KB	6/30/2015 4:59 PM

Chrome 42 fixes >40 vulnerabilities and disables NPAPI support.

- NPAPI: Netscape Plugin Application Programming Interface
- A plug-in architecture to allow add-ons to handle additional content types.
- Google has been warning of this for some time. The time has come:
- Until Chrome 45 (September 2015) it CAN still be enabled manually, but Chrome 45 REMOVES it.
  - chrome://flags/#enable-npapi
  - JAVA and Silverlight
- Chrome's FLASH support uses it's own extender "Pepper" PPAPI.
- Safari & Firefox continue to support NPAPI, IE briefly did, but dropped it way back in v5.5.

Popular 3rd-Party HTTPS library had a bad problem...

- AFNetworking -- open-source drop-in networking for iOS apps
- v2.5.1, released in January, skips certificate verification checks.
- v2.5.2, 3-weeks ago the code maintainers found and fixed the flaw.
- At least 1500 iOS Apps in 2 million installations remain vulnerable.
- Any simple web proxy is able to intercept and decrypt all traffic since its cert is never checked.
- Examples are:
  - Citrix OpenVoice Audio Conferencing
  - Alibaba.com mobile app

    - Movies by Flixster with Rotten Tomatoes
    - KYBankAgent 3.0
    - Revo Restaurant Point of Sale

- SourceDNA:
    - Identified vulnerable apps by scanning all free titles and the top 5,000 for-fee titles available for download in Apple's App Store and analyzing the binary code in each one.
- Approx 1 million of the 1.4 million titles in the App Store were analyzed.
- The 1,500 vulnerable apps are those that:
    - use AFNetwork version 2.5.1
    - use HTTPS
    - don't implement certificate pinning
- The 1,500 apps identified don't include those that were fixed after SourceDNA privately reported the vulnerability to developers. App developers who fixed the bug include companies such as Yahoo, Microsoft, and Uber.
- Search Tool to check for vulnerable iOS Apps…
    - http://searchlight.sourcedna.com/lookup

"Let's Encrypt" Moves Forward:

- Recap: https://letsencrypt.org/
    - It's a new Certificate Authority
    - Free, Automated & Open.
    - Arrival targeted at mid-2015.
    - Issue two commands:
        - $ sudo apt-get install lets-encrypt
        - $ lets-encrypt example.com
- Until now... the process of proving domain control and obtaining a certificate was 100% manual. "Let's Ecrypt" is a simple protocol that:
    - Automatically prove to the Let’s Encrypt CA that you control the website
    - Obtain a browser-trusted certificate and set it up on your web server
    - Keep track of when your certificate is going to expire, and automatically renew it
    - Help you revoke the certificate if that ever becomes necessary.
- And... it's 100% FREE!

- Today's News: NCC group (who just finished the TrueCrypt audit) is now engaged
    - https://letsencrypt.org/2015/04/14/ncc-group-audit.html
- Bounder:
    - Let’s Encrypt’s CA (backend) software is called boulder.
    - Mostly written in the GO language.
    - Boulder contains modules including a web front-end and registration, validation, certificate, and storage authorities.
- ACME:
    - ACME, short for Automated Certificate Management Environment
    - Protocol Let’s Encrypt will use for automatic certificate issuance and management.
    - Hope to make ACME an IETF standard.

Miscellany:

Twitter allows optional DMs from anyone:

- Security & Privary / Privacy (section) / Direct Messages: "Receive Direct Messages from anyone"
- I've turned it ON!

SQRL News:

- Thrashing out the last bits of the protocol: Enable/Disable/Remove.
- Stina - Yubico + SQRL.
- U2F - Universal Second Factor
    - FIDO -- cannot be secure single factor auth.
    - It can only CONFIRM that you are who you first claim to be.
- SQRL and federated authentication.

SpinRite

Andre Couture (@nomade1999) 2:43pm · 16 Apr 2015 · iOS
@SGgrc spinrite just saved my wife's school computer! Your latest podcast just clarified some of those numbers I saw.

Great Firewalls & Cannons

CitizenLab: https://citizenlab.org/2015/04/chinas-great-cannon/

- http://techcrunch.com/2015/04/10/china-great-cannon/
- http://www.usnews.com/news/articles/2015/04/14/chinas-great-cannon-redirects-us-traffic-for-censorship
- http://phys.org/news/2015-04-roar-china-great-cannon-heard.html
- http://www.adweek.com/socialtimes/chinese-great-cannon-uses-ddos-style-redirects-for-censorship/618871
- http://fortune.com/2015/04/13/china-has-weaponized-its-internet-with-the-great-cannon/
- http://www.theguardian.com/technology/2015/apr/13/great-cannon-china-internet-users-weapon-cyberwar
- http://www.nytimes.com/2015/04/11/technology/china-is-said-to-use-powerful-new-weapon-to-censor-internet.html

What is the Great Firewall and how does it work?

- Located in the data centers of China's four major ISPs to filter Internet traffic coming into China.
- Not a Man-In-The-Middle... a "Man On The Side"
- A "monitoring tap" that watches all non-secured HTTP traffic.
- When any "Banned Content" is seen, the firewall sends TCP/RST packets to both endpoints.
- SYN, SYN/ACK, ACK ... FIN, FIN/ACK, ACK.
    - Graceful shutdown vs abortive shutdown.

Last month, in mid-March of 2015, something unprecedented occurred:

- An apparently state-sponsored and VERY PUBLIC attack was launched against two Github sites which offered censorship circumvention software solutions.
- China had once previously blocked access to the entire Github domain, but the outcry from Chinese software developers over the loss of Github ended the domain block in two days.
- The Chinese censors needed a finer-grained filter. But since Github uses HTTPS, the Great Firewall cannot see into those connections to block access to specific parts of Github.
- So... someone had the idea to attack those specific pages.

What is the Great Cannon and how does it work?

- The "Great Cannon" is an active offensive cyberweapon.
- It IS a "Main In The Middle" attack tool.
- It reads some portion (apparently not all) of incoming non-secured web queries.
- Based upon selection criteria, it intercepts some queries and returns alternative content to the requester.
- This could be any payload the Chinese government chooses.
    - While this is requests *TO* an IP, it could also be requests *FROM* an IP.
    - ANY query from a specific user to any web asset inside China could result in altered content.
- In the case of this very public attack, it returned a JavaScript file which caused the user's web browser to overload specific Github properties with queries.

Who launched the attack?

- Traceroutes tell the story:
    - While the attack was underway, many people were curious to learn as much as they could.
    - From many different locations around the globe, crossing into China through different widely spaced carriers, the "hop counts" to the Great Firewall and the Great Cannon... were identical.
    - They had to be co-located at the same routers.
- Also…
    - The packets being emitted by BOTH the Great Firewall and the Great Cannon display an oddity in their own outbound TTLs... which is unique and identical, strongly suggesting, at least, a common code base.

What does all this portend for the future?

- Encryption is "annoying" everyone except its users.
- The inability to see into web traffic is becoming increasingly troublesome to those who want to see in.