Security Now! #515 - 07-07-15

A Crazy News Week!

This week on Security Now!

- Firefox v39
- ICANN's WHOIS privacy policy
- A new old DDoS attack protocol in use
- Amazon rolls their own TLS stack
- ARIN runs out of IPv4 space
- Italy's Hacking Team gets hacked... with a surprise in the disclosed data!
- Juicy new details about the NSA's XKEYSCORE and International spying
- Windows 10 gets privacy-worrisome "WiFi Sense" facility.
- And more!!

Security News

Firefox v39

- https://www.mozilla.org/en-US/firefox/39.0/releasenotes/
- SafeBrowsing malware detection has been added to Mac OS X & Linux. (Oh, joy.)
  - (Uses Google SafeBrowsing info to detect if downloads are malicious.)
  - The malware detection service for downloads now covers common Mac file types.
- Firefox "Hello" (real-time chat component) Hello URL sharing on social media.
- Architecture:
  - Asynchronous Plug-in Initialization - Plug-in Init used to be synchronous and could hang Firefox startup. Now plug-ins are launched asynchronously.
- Removed support for insecure SSLv3 for network communications.
- Disable use of RC4 except for temporarily whitelisted hosts.
- 13 security-related bug fixes.
- Increasing support for the more obscure HTML5 features.

- Alex Neihaus (@yobyot) 7/6/15, 8:21 AM
  - (ex-VP Marketing, Astaro Corp.)
  - @SGgrc After years of avoiding it, switching to #Firefox+#NoScript from #Chrome. It hurts so good. Not recommended for the faint of heart.

- (A reminder/note about "MailStore Home 8" by MailStore:)
  - "MailStore Home" is FREE for non-commercial usage.
  - http://www.mailstore.com/en/mailstore-home-email-archiving.aspx

ICANN's plans for WHOIS privacy

- https://gnso.icann.org/en/issues/raa/ppsai-initial-05may15-en.pdf
- OMG! 98-pages of bureaucratic double-speak!
- "Initial Report on the Privacy & Proxy Services Accreditation Issues Policy Development Process"
- Section 1.3: WG Preliminary Recommendations
    - Section 1.3.1: Summary of the WG's agreed preliminary conclusions
    - II. NO DISTINCTION IN TREATMENT; WHOIS LABELING REQUIREMENTS; VALIDATION & VERIFICATION OFCUSTOMER DATA:
        - 2. Privacy and proxy services ("P/P services") are to be treated the same way for the purpose of the accreditation process.
        - 3. The status of a registrant as a commercial organization, non-commercial organization, or individual should not be the driving factor in whether P/P services are available to the registrant. Fundamentally, P/P services should remain available to registrants irrespective of their status as commercial or non-commercial organizations or as individuals. Further, P/P registrations should not be limited to private individuals who use their domains for non-commercial purposes (Note10)
        - Note 10: Note that while the WG agreed that there is no reason to distinguish between commercial and non-commercial registrants simply because of their organizational/entity status, it has not reached consensus as to whether the use of P/P services for certain types of commercial activity associated with a domain name should be barred (see Section 1.3.3 and more generally Section 7, below).

    - 1.3.3 Specific topics on which there is currently no consensus within the WG
      Although the WG agreed that the mere fact that a domain name is registered by a commercial entity or by anyone conducting commercial activity should not preclude the use of P/P services, there was disagreement over whether domain names that are actively used for commercial transactions (e.g. the sale or exchange of goods or services) should be prohibited from using P/P services. While most WG members did not believe such a prohibition is necessary or practical, some members believed that registrants of such domain names should not be able to use or continue using P/P services.

      For those that argued that it is necessary and practical to limit access to P/P services so as to exclude commercial entities, the following text was proposed to clarify and define their position: "domains used for online financial transactions for commercial purpose should be ineligible for privacy and proxy registrations."

      Public comment is therefore specifically invited on the following questions:
        - Should registrants of domain names associated with commercial activities and which are used for online financial transactions be prohibited from using, or continuing to use, P/P services? If so, why, and if not, why not?
        - If you agree with this position, do you think it would be useful to adopt a definition of "commercial" or "transactional" to define those domains for which P/P service registrations should be disallowed? If so, what should the definition(s) be?

        - Would it be necessary to make a distinction in the WHOIS data fields to be displayed as a result of distinguishing between domain names used for online financial transactions and domain names that are not?

- Google's Adam Langley:
    - https://www.imperialviolet.org/2015/07/05/icannwhois.html
    - Analyzed the reply eMail (which is all public) and found that approximately 90% of the posted replies were in favor of NOT EXCLUDING commercial entities (whatever they are) from the privacy afforded by WHOIS proxying.

The new DDoS protocol target: RIPv1

- Background:
    - Unlike TCP, UDP protocols are generally vulnerable to IP spoofing reflection attacks since the endpoint IPs are never verified.
    - The last bandwidth amplification attack was NTP, and before that, DNS.
- Now we're seeing the use of RIPv1...
- http://www.networkworld.com/article/2943873/attackers-abuse-legacy-routing-protocol-to-amplify-distributed-denialofservice-attacks.html
- Network World writes:
    - DDoS attacks observed in May by the research team at Akamai abused home and small business (SOHO) routers that still support Routing Information Protocol version 1 (RIPv1). This protocol is designed to allow routers on small networks to exchange information about routes.

      In the DDoS attacks seen by Akamai, which peaked at 12.8 gigabits per second, the attackers used about 500 SOHO routers that are still configured for RIPv1 in order to reflect and amplify their malicious traffic.

- Old RIPv1 protocol still available.
    - MANY routers still support RIPv1
- UDP port 520
- Version 1:
    - RFC 1058, published 27 years ago in 1988.
    - Only "classful" network representation (no CIDR support), no variable length subnet masks.
    - NO ROUTER AUTHENTICATION!

- Version 2:
    - Developed in in the eary-mid 90's and standardized in 1998 (RFC 2453).
    - Added the ability to carry subnet information, so supports CIDR.

- What makes this powerful is that DNS and NTP servers tend to be professionally managed and supervised. And when abuse is detected their IT staff lock them down.
- But SOHO routers with RIPv1 exposed to the Internet are unsupervised.

Amazon releases their "s2n" TLS stack. It's on Github.

- https://blogs.aws.amazon.com/security/post/TxCKZM94ST1S6Y/Introducing-s2n-a-New-Open-Source-TLS-Implementation
- s2n -- "signal to noise"
- At Amazon Web Services, strong encryption is one of our standard features, and an integral aspect of that is the TLS (previously called SSL) encryption protocol. TLS is used with every AWS API and is also available directly to customers of many AWS services.

  Part of the challenge is that the TLS protocol, including all of its optional extensions, has become very complex. OpenSSL, the de facto reference implementation, contains more than 500,000 lines of code with at least 70,000 of those involved in processing TLS. Naturally with each line of code there is a risk of error, but this large size also presents challenges for code audits, security reviews, performance, and efficiency.

  In order to simplify our TLS implementation and as part of our support for strong encryption for everyone, we are pleased to announce availability of a new Open Source implementation of the TLS protocol: s2n. s2n is a library that has been designed to be small, fast, with simplicity as a priority. s2n avoids implementing rarely used options and extensions, and today is just more than 6,000 lines of code. As a result of this, we've found that it is easier to review s2n; we have already completed three external security evaluations and penetration tests on s2n, a practice we will be continuing.

  Over the coming months, we will begin integrating s2n into several AWS services. TLS is a standardized protocol and s2n already implements all the functionality we use, so this won't require any changes in your own applications and everything will remain interoperable.

  If you are interested in using or contributing to s2n, the source code, documentation, commits and enhancements are all publically available under the terms of the Apache Software License 2.0 from the s2n GitHub repository.

Last Wednesday night ARIN (for the first time ever) ran out of IPv4 space and declined a request (Wed, July 1st, 2015)

- https://www.arin.net/announcements/2015/20150701.html
- ARIN activated the "IPv4 Unmet Requests policy (NRPM 4.1.8)" this week with the approval of an address request that was larger than the available inventory in the regional IPv4 free pool. Full details about this process are available at:
- https://www.arin.net/resources/request/waiting_list.html
    - When ARIN receives a justified request for IPv4 address space that cannot be filled by a single block from ARIN's available IPv4 free pool, the requestor will have three options:
    - Accept the largest available block in the ARIN IPv4 free pool that is equal to or less than your approved size. ARIN will fill the request per ARIN policy and the requestor will then be ineligible to receive IPv4 addresses from the ARIN IPv4 free pool for the next three months.
    - Elect not to accept an available block from the ARIN IPv4 free pool and request to be put on the Waiting List for Unmet Requests. ARIN will ask you to specify the

smallest block size you are willing to accept and will place your request on the waiting list for a range that includes your approved size through the minimum size you designated. This procedure is in accordance with ARIN's Number Resource Policy Manual (NRPM) Section 4.1.8.
    - Elect not to accept an available block from the ARIN IPv4 free pool and close out the request.

- How the Waiting List for Unmet Requests Works
    - When an IPv4 block becomes available, the oldest waiting list request that has specified a minimum acceptable block size equal to or less than the available block will be filled and the request will be removed from the waiting list. ARIN will re-verify the organization's justified need to make sure nothing with regard to the organization's justification for resources has materially changed since the original request was approved.

- ARIN does still have limited amounts of IPv4 address space available in smaller block sizes. We encourage customers to monitor the IPv4 Inventory Counter on the ARIN homepage and the breakdown of the remaining IPv4 inventory found on our IPv4 Depletion page:
    - https://www.arin.net/resources/request/ipv4_countdown.html

- Organizations that need larger amounts of address space are encouraged to make use of the IPv4 transfer market for those needs. ARIN also reminds organizations of the ample availability of IPv6 address space, and encourages organizations to evaluate IPv6 address space for their ongoing public Internet network activities.

- How much does ARIN have left?
    - 46 remaining /23's (512-IP block) --- Now: 39!
    - 431 remaining /24's (256-IP block) --- Now: 424

- The Countdown Plan has four phases, and ARIN is currently in Phase Four:
    - Phase One began in February 2011 when ARIN received its last /8 from IANA.
    - Phase Two began in September 2012 when ARIN reached three remaining /8 equivalents.
    - Phase Three began in August 2013 when ARIN reached two remaining /8 equivalents.
    - Phase Four began in April 2014 when ARIN reached one remaining /8 equivalent.

- IPv6 Depletion?
    - https://samsclass.info/ipv6/exhaustion.htm
    - (Required script... and is slowly counting down.)

Hacking Team Hacked (revealed Sunday)

- http://www.csoonline.com/article/2943968/data-breach/hacking-team-hacked-attackers-claim-400gb-in-dumped-data.html
- http://www.csoonline.com/article/2944333/data-breach/hacking-team-responds-to-data-breach-issues-public-threats-and-denials.html

- 400GB of data placed on a Torrent.
- Twitter acct taken over, (unimpressive) passwords published.
- They're not taking it very well: Threatening, accusing, and denying clear facts.
- WIRED: "The FBI Spent $775K on Hacking Team's Spy Tools Since 2011"
- http://www.wired.com/2015/07/fbi-spent-775k-hacking-teams-spy-tools-since-2011/
- Private Italian spying software provider.
- Has sold their products, indiscriminantly to suppressive regimes
- "RCS" - Remote Control Service - aka "Galileo" - their premiere spying product.
- Standard RAT - Remote Access Trojan:
    - Siphons off data & intercepts communications before they have been encrypted.
    - Record Skype calls, e-mails, instant messages, and passwords typed into a Web browser.
    - Can switch on a target's webcam & microphone.
- "Hacking Team" maintains an office in the US.
    - A US government contractor "Cicom USA" has the same phone number and address.
    - FBI and DEA have purchased surveillance technology, maintenance agreements, license renewals from CICOM USA.
- Note that the US Congress has never explicitly granted any law enforcement agencies the legal authority to hack anyone's computers.

Previously unknown FLASH 0-day FOUND AMONG the Hacking Team documents!!

- http://www.kb.cert.org/vuls/id/561288
- https://twitter.com/w3bd3vil/status/618168863708962816
    - (Tweet contains a link to the exploit code.)

A Look at the Inner Workings of NSA's XKEYSCORE

- https://firstlook.org/theintercept/2015/07/02/look-under-hood-xkeyscore/
- https://www.schneier.com/blog/archives/2015/07/more_about_the_.html
- 48 Classified documents released by "The Intercept" Sunday.

- The System:
    - XKEYSCORE is Linux software running on Red Hat servers which run Apache and MySQL.
    - File systems are clustered NFS file system running the autofs service.
    - CRON runs the system's scheduled tasks.
    - Admins connect with SSH and use rsync and vim to manage the software.
    - Analysts connect to XKEYSCORE over HTTPS using standard web browsers such as Firefox. IE is not supported.
    - Analysts log into the system with either a user ID and password or by using public key authentication.
    - "Micro-plugins" analyze and tag all incoming traffic with various AppIDs to classify the traffic.
    - A custom programming language "Genesis" allows new tagging filters to be created.
    - A single query is replicated to query all sites simultaneously.
- As of 2009:

    - Approximately 150 global sites & more than 700 servers (6 or 7 years ago).
    - Variable size clusters depending upon the traffic volume and processing needed.
    - In 2009, Some sites receive >20 TB/day.

- Quote by John Adams, former security lead and senior operations engineer for Twitter: "One of the most interesting things about XKEYSCORE's architecture is that they have been able to achieve so much success with such a poorly designed system. Data ingest, day-to-day operations, and searching is all poorly designed. There are many open source offerings that would function far better than this design with very little work. Their operations team must be extremely unhappy."

- "The Intercept" article contains links to the trove of documents.

WikiLeaks publishes details of NSA intercepts of German government communications

- Spreadsheet of the intelligence targets:
- https://www.wikileaks.org/nsa-germany/selectors.html
- Bruce Schneier writes:
    - https://www.schneier.com/blog/archives/2015/07/nsa_german_inte.html
    - <quote> On Friday, WikiLeaks published three summaries of NSA intercepts of German government communications. To me, the most interesting thing is not the intercept analyses, but the spreadsheet of intelligence targets. Here we learn the specific telephone numbers being targeted, who owns those phone numbers, the office within the NSA that processes the raw communications received, why the target is being spied on (in this case, all are designated as "Germany: Political Affairs"), and when we started spying using this particular justification. It's one of the few glimpses we have into the bureaucracy of surveillance.
- Other similar recent Wikileaks reveals for France and Brazil in the past week.
- Der Spiegel is also VERY unhappy:
    - http://www.spiegel.de/international/germany/the-nsa-and-american-spies-targeted-spiegel-a-1042023.html
    - <quote> Revelations from WikiLeaks published this week show how boundlessly and comprehensively American intelligence services spied on the German government. It has now emerged that the US also conducted surveillance against SPIEGEL.

Window's new "WiFi Sense" shares your WiFi password with Facebook, Outlook & Skype contacts

- http://www.extremetech.com/extreme/209208-windows-10s-new-wifi-sense-shares-your-wifi-password-with-facebook-outlook-and-skype-contacts
- https://www.windowsphone.com/en-us/how-to/wp8/connectivity/wi-fi-sense-faq
- Unclear whether it's default ON or not.

- *Microsoft's FAQ reads:*
  "When you share Wi-Fi network access with Facebook friends, Outlook.com contacts, or Skype contacts, they'll be connected to the password-protected Wi-Fi networks that you choose to share and get Internet access when they're in range of the networks (if they

use Wi-Fi Sense). Likewise, you'll be connected to Wi-Fi networks that they share for Internet access too. Remember, you don't get to see Wi-Fi network passwords, and you both get Internet access only. They won't have access to other computers, devices, or files stored on your home network, and you won't have access to these things on their network."

- Elsewhere in the FAQ, Microsoft notes that if you choose to share this information, it is sent via an encrypted link to Microsoft, who stores the data on their own servers.

- *Extreme Tech notes:*
  <quote> The other concern we have with WiFi Sense is that the feature has no granularity beyond the service level. I can choose to share or not-share information with Facebook, Outlook, or Skype, but that's it. If you share your network information with anyone on your Facebook friends list, you're sharing it with everyone on your Facebook friends list. That's something Microsoft really ought to have addressed when it brought the feature over from Windows Phone; just because I want to share this kind of data with some people doesn't mean I want to share it with everyone.

TLS Client Puzzles Extension - Bitcoin cleverness heads toward TLS v1.3

- Akamai Technologies, July 02, 2015
- https://www.ietf.org/id/draft-nygren-tls-client-puzzles-00.txt
- Essentially, SHA256, SHA512, and memory-hard puzzles the client must solve.

PrivacyTools.io

- Why do there recommendations differ from SN's?
- Threema is closed source.
- LastPass uses cloud sync and has been attacked in the past.
- "We don't recommend closed source / US / Cloud based password managers since great alternatives exist"

A bit of humor:

- Chris Wronski (@theemptyset)
- @SGgrc @leolaporte I just solved the settlement free peering problem! Netflix merges w/Carbonite. You're welcome.

Ron Houk, tweets via (@archhouk):

Steve, have you checked out the advanced options of ublock origin? They're pretty nice! Go to plug-in dashboard and check the "I am an advanced user" checkbox. Then, back on your toolbar, when you click on the ublock icon. There'll be plus signs (+) to the left of "Requests blocked" and "Domains connected" which opens a very nice details display!

Hoodie, tweeting via (@hoodie_de)

Hi, You praised web assembly pretty highly. Could you go into its security implications? Thank you!