Security Now! #443 - 02-18-14

Sisyphus

Link Tracking Warning!

This document was first authored in Google Docs, then Downloaded as a PDF. So, Google has thoughtfully (ha!) added "tracking" redirections to all of the links here. (I have no idea why, but that's Google.) If that bothers you, simply copy the text of the link into your browser's URL field.

This Week on Security Now!

- A tiny tweak to Firefox
- Kickstarter's data exfiltration
- Thoughts about the new MEGA DDoS attacks,
- Bitcoin Protocol Troubles,
- CryptoLocker Greed
- Google's Authentication purchase,
- Linksys routers propagating a worm,
- Asus routers sharing their files on the internet,
- Belkin's WeMo does Mo than you probably want,
- Some Sci-Fi updates,
- Something you can see of SQRL,

SpinRite:

- John Woods @JohnAlanWoods / 1:26pm · 13 Feb 14 · web
- @SGgrc just used Spinrite 6. Incredible, what a fantastic tool. Files are back!

Firefox v27.0.1

- https://www.mozilla.org/en-US/firefox/27.0.1/releasenotes/
- FFv27 released on 2/4/2014
- TLS v1.1 and v1.2 -- both enabled by default.)
- Added support for SPDY v3.1.

Security News...

Kickstarter Breach

https://www.kickstarter.com/blog/important-kickstarter-security-notice

- Yancey Strickler (Cofounder/Head of Communications at Kickstarter), Saturday 2/15:
- On Wednesday night, law enforcement officials contacted Kickstarter and alerted us that hackers had sought and gained unauthorized access to some of our customers' data. Upon learning this, we immediately closed the security breach and began strengthening security measures throughout the Kickstarter system.

  No credit card data of any kind was accessed by hackers. There is no evidence of unauthorized activity of any kind on all but two Kickstarter user accounts.

  While no credit card data was accessed, some information about our customers was. Accessed information included usernames, email addresses, mailing addresses, phone numbers, and encrypted passwords. Actual passwords were not revealed, however it is possible for a malicious person with enough computing power to guess and crack an encrypted password, particularly a weak or obvious one.

  Q: How were passwords encrypted?
  A: Older passwords were uniquely salted and digested with SHA-1 multiple times. More recent passwords are hashed with bcrypt.

400 gbps NTP reflection attack

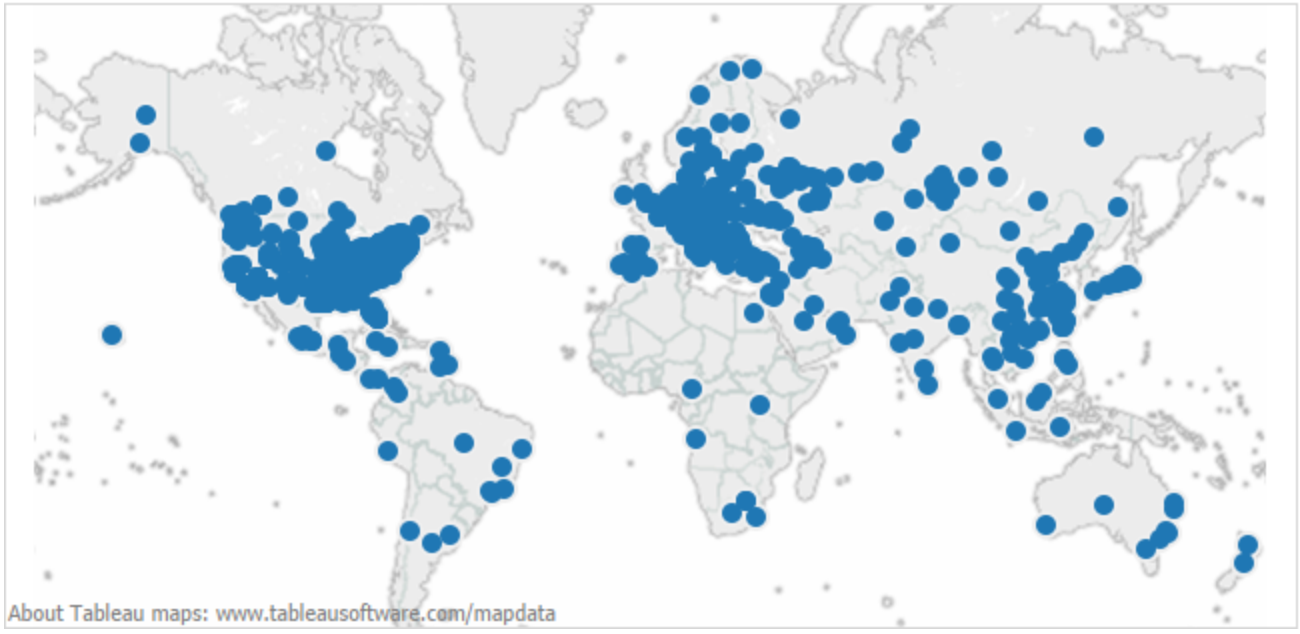
- Previous record DDoS was 300gbps
- Relative size of various NTP attacks:
  - https://www.us-cert.gov/ncas/alerts/TA14-017A
- http://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack
- "Not Just Theoretical":

  Monday's DDoS proved these attacks aren't just theoretical. To generate approximately 400Gbps of traffic, the attacker used 4,529 NTP servers running on 1,298 different networks. On average, each of these servers sent 87Mbps of traffic to the intended victim on CloudFlare's network. Remarkably, it is possible that the attacker used only a single server running on a network that allowed source IP address spoofing, to initiate the requests.

  While NTP servers that support MONLIST are less common than open DNS resolvers, they tend to run on beefier servers with fatter connections to the network. Combined with the high amplification factor, this allows a much smaller number of NTP servers to generate very large attacks. For comparison, the attack that targeted Spamhaus used 30,956 open DNS resolvers to generate a 300Gbps DDoS. On Monday, with 1/7th the number of vulnerable servers, the attacker was able to generate an attack that was 33% larger than the Spamhaus attack.

- John Graham-Cumming:
  http://blog.cloudflare.com/understanding-and-mitigating-ntp-based-ddos-attacks

- The problem of "Proximity Congestion"



Linksys Router "The Moon" Worm:

- Brett Glass -- who operates a Wyoming-based ISP.
  <<< share Brett's Note >>>
- http://arstechnica.com/security/2014/02/bizarre-attack-infects-linksys-routers-with-self-replicating-malware/?comments=1&post=26233825#comment-26233825
- Malware contains HTML pages and images from the movie "The Moon".
- The worm works by injecting vulnerable devices with a URL-encoded shell script that carries out the same seek-and-hijack behavior.
- http://windowsitpro.com/security/self-replicating-worm-actively-attacking-linksys-routers
- http://arstechnica.com/security/2014/02/bizarre-attack-infects-linksys-routers-with-self-replicating-malware/
- http://windowsitpro.com/security/update-linksys-router-worm-fix-and-further-actions
- Models: E4200, E3200, E3000, E2500, E2100L, E2000, E1550, E1500, E1200, E1000, E900
- Connects to port 8080, runs a CGI script on the router which downloads and executes a 2 MB program which scans for other vulnerable routers -- lives only in RAM. Reboot clears.
- Official Statement:
  "Linksys is aware of the malware called "The Moon" that has affected select older Linksys E-Series routers and select older Wireless-N access points and routers. The exploit to bypass the admin authentication used by the worm only works when the Remote Management Access feature is enabled. Linksys ships these products with the Remote Management Access feature turned off by default. Customers who have not enabled the Remote Management Access feature are not susceptible to this specific malware. Customers who have enabled the Remote Management Access feature can prevent further vulnerability to their network, by disabling the Remote Management Access feature and rebooting their router to remove the installed malware. Linksys will be working on the affected products with a firmware fix that is planned to be posted on our website in the coming weeks."

- Linksys Knowledgebase: (http://bit.ly/themoonworm)
  The Moon malware bypasses authentication on the router by logging in without actually knowing the admin credentials. Once infected, the router starts flooding the network with ports 80 and 8080 outbound traffic, resulting in heavy data activity. This can be manifested as having unusually slow Internet connectivity on all devices.

BELKIN -- Speak of the devil:

- http://beta.slashdot.org/story/198331
- What is "WeMo" ??
  - http://www.belkin.com/us/Products/home-automation/c/wemo-home-automation/
  - Lightswitches, Outlet plugs, Motion Detectors
  - Partnering with Mr.Coffee, CrockPot, Sunbeam, and others "to bring home automation to your favorite everyday appliances."
  - <quote> You'll be able to turn that device on or off using your smartphone or tablet (running Android 4.0 and later or iOS 5 or higher) from anywhere. The WeMo Switch uses your existing home Wi-Fi network to provide wireless control of TVs, lamps, stereos, heaters, fans and more.
- Over half a million WeMo users.
- http://www.ioactive.com/news-events/IOActive_advisory_belkinwemo_2014.html
- http://www.ioactive.com/pdfs/IOActive_Belkin-advisory-lite.pdf
- <quote> (Today: February 18th)
  IOActive, Inc., the leading global provider of specialist information security services, announced today that it has uncovered multiple vulnerabilities in Belkin WeMo Home Automation devices that could affect over half a million[1] users. Belkin's WeMo uses Wi-Fi and the mobile Internet to control home electronics anywhere in the world directly from the user's smartphone.

  Mike Davis, IOActive's principal research scientist, uncovered multiple vulnerabilities in the WeMo product set that gives attackers the ability to:

  • Remotely control WeMo Home Automation attached devices over the Internet
  • Perform malicious firmware updates
  • Remotely monitor the devices (in some cases)
  • Access an internal home network

  Davis said, "As we connect our homes to the Internet, it is increasingly important for Internet-of-Things device vendors to ensure that reasonable security methodologies are adopted early in product development cycles. This mitigates their customer's exposure and reduces risk. Another concern is that the WeMo devices use motion sensors, which can be used by an attacker to remotely monitor occupancy within the home."

  Once an attacker has established a connection to a WeMo device within a victims network; the device can be used as a foothold to attack other devices such as laptops, mobile phones, and attached network file storage.

- Details:
- For some reason, the firmware's signing key is INCLUDED in the firmware!
  The Belkin WeMo firmware images that are used to update the devices are signed with public key encryption to protect against unauthorised modifications. However, the signing key and password are leaked on the firmware that is already installed on the devices. This allows attackers to use the same signing key and password to sign their own malicious firmware and bypass security checks during the firmware update process.

- SSL *only* used for privacy, not for authentication! (Whoops!!)
  Belkin WeMo devices do not validate Secure Socket Layer (SSL) certificates preventing them from validating communications with Belkin's cloud service including the firmware update RSS feed. This allows attackers to use any SSL certificate to impersonate Belkin's cloud services and push malicious firmware updates and capture credentials at the same time. Due to the cloud integration, the firmware update is pushed to the victim's home regardless of which paired device receives the update notification or its physical location.

- NAT traversing "STUN" and "TURN" protocols can be abused:
  The Internet communication infrastructure used to communicate Belkin WeMo devices is based on an abused protocol that was designed for use by Voice over Internet Protocol (VoIP) services to bypass firewall or NAT restrictions. It does this in a way that compromises all WeMo devices security by creating a virtual WeMo darknet where all WeMo devices can be connected to directly; and, with some limited guessing of a 'secret number', controlled even without the firmware update attack.

- Finally…
  The Belkin WeMo server application programming interface (API) was also found to be vulnerable to an XML inclusion vulnerability, which would allow attackers to compromise all WeMo devices.

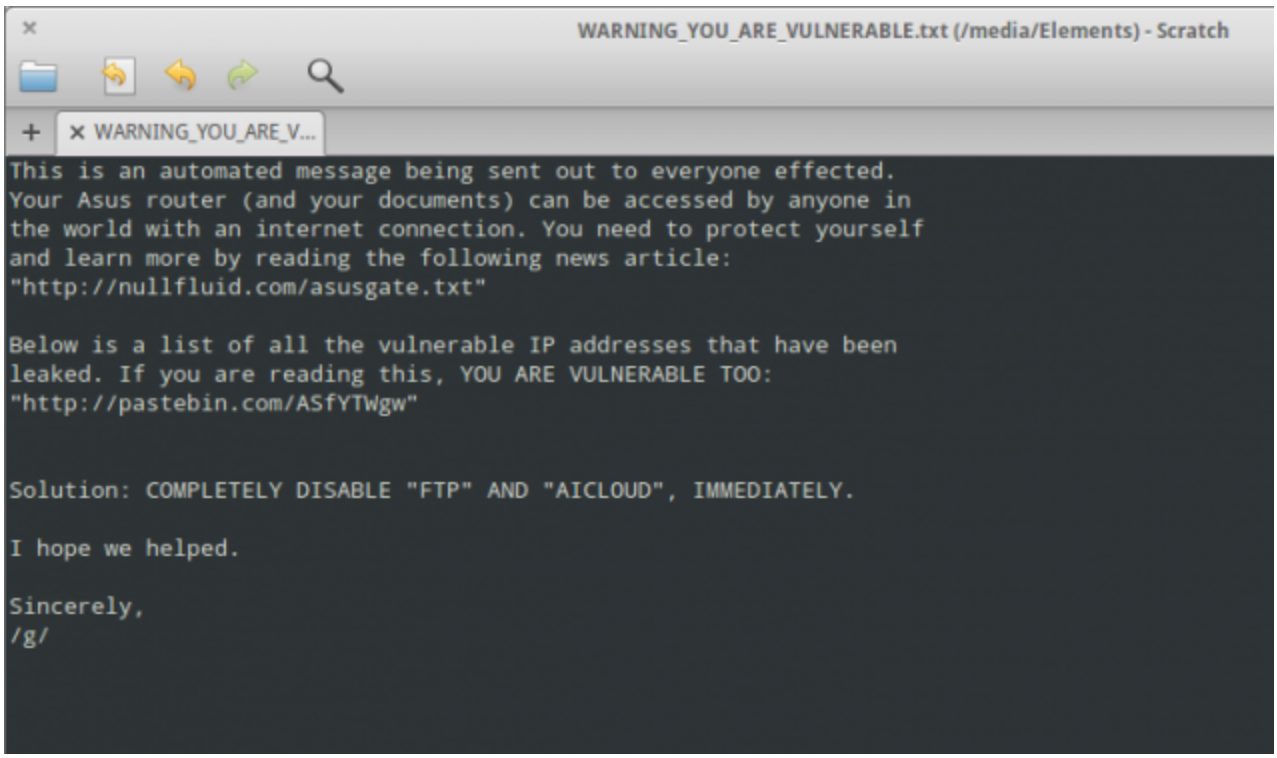
- Responsible Disclosure:
  IOActive feels very strongly about responsible disclosure and as such worked closely with CERT on the vulnerabilities that were discovered. CERT, which will be publishing its own advisory today, made several attempts to contact Belkin about the issues, however, Belkin was unresponsive.

  Due to Belkin not producing any fixes for the issues discussed, IOActive felt it important to release an advisory and recommends unplugging all devices from the affected WeMo products.

ASUS Routers Exposing their connected drive's contents to the Internet

- http://arstechnica.com/security/2014/02/dear-asus-router-user-youve-been-pwned-thanks-to-easily-exploited-flaw/
- ASUS http://nullfluid.com/asusgate.txt
  - ASUSTeK Computer Inc (ASUS) have spent the better part of a year ignoring the fact that their RT-series routers suffer from two CRITICAL security vulnerabilities.
    - 1. Default setting for the ftp-server was to allow anonymous login. ASUS calls this feature "limitless access rights." We call this madness.

        - 2. AiCloud usernames and passwords were stored in plaintext in a file available for download without logging in. We call this insanity.
    - Not only did they ship RT-routers with these vulnerabilities and ignore Kyle Lovetts emails and phonecalls informing them about them. They also failed to provide firmware upgrades where these vulnerabilities were removed for another SIX months. Did they even perform security audits on their products before releasing them? Considering the use of plain-text storage of login credentials we have a really hard time believing they did.
    - This is not rocket surgery. Anyone with the slightest knowledge or interest in "security" would know this is unforgivable.
    - Vulnerability #1 (FTP) gives EVERYONE on the internet access to attached USB storage making it possible to download and upload files. You do not need an untamed imagination to realize the implications this has.



- Kyle Lovetts, June 22nd Bug report: http://www.securityfocus.com/archive/1/526942

- Timeline:
  - Contacted Asus two weeks ago (under my online handle account) around 06/06
  - Second email send on 06/10 when discovered first un-authenticated file disclosure
  - Received only one response back stating it was not an issue
  - Sent a third email on 06/14
  - Only response received was an acknowledgement that my email was received
  - Attempted to call their development or incident team, and was told that someone would call me back on 06/17
  - Sending another email today under my real name

- Mitigation and temporary fixes:
  - Users need to be alerted to turn off AiCloud service immediately
  - All Web access to both the http and https need to be halted until proven safe
  - UPnP services need to be turned off (I'd say that a safe bet is for all home routers to turn it off)
  - Disable FTP and Samba services until the problem is fully understood/patched if possible
  - Enable the built in firewall, change authentication to be MD5 hashed
  - CHANGE THE DEFAULT USERNAME AND PASSWORD!!!!
  - End Users should try to avoid using the default gateway of 192.168.1.1 and pick something unusual
  - Turn off IPSEC, PPTP and the other NAT passthroughs if the VPN is not explicitly being utilized
  - Upgrade to third party firmware, which appears from a few reports to be immune to some extent (not proven or tested)

SlickLogin

- http://www.securityweek.com/google-acquires-authentication-sound-startup-slicklogin
- http://techcrunch.com/2013/09/09/slicklogin-wants-to-kill-the-password-by-singing-a-silent-song-to-your-smartphone/
- http://www.slicklogin.com/

- Google purchased three smart guys and one or more patents
- "Add just 5 lines of code to your web app" means that, in addition to whatever else, it's a 3-party solution. Trust them??

Google Mail peeking inside "infected" ZIPs

- http://www.ghettoforensics.com/2014/02/google-actively-scanning-malware-emails.html
- Malware researcher Brian Baskin was exchanging Encrypted-ZIP malware... Google Noticed! Then subsequently remembers the filename even if the password is changed.

CryptLocker getting Greedy!

- Newest CryptoLocker demands payment of 5 bitcoins!
- Once it was ~$300. Today? $3,000 (5 x $600 USD)

"Transaction Malleability" in the Bitcoin Protocol

- http://spectrum.ieee.org/tech-talk/computing/networks/what-you-need-to-know-about-mt-gox-and-the-bitcoin-software-flaw
- Timing Hack due to the transaction confirmation delay.
- IEEE Spectrum writes:
- <quote> In order to understand transaction malleability, you need to know that the balances of all Bitcoin addresses are maintained on a public ledger and that the changes made to this ledger are what constitute the transfer of funds.

When a transaction is broadcast to the network, it is relayed with a digital fingerprint that identifies it. Bitcoin miners then scoop it up, verify it, and send it on to the rest of the network for confirmation. Once the transaction has been confirmed, there is no way for that same person to spend those same bitcoins because they are being checked against the public ledger.

The malleability feature allows a person to intervene, right after the transaction request has been sent, modify the fingerprint and create a duplicate transaction. So, now you have two unconfirmed transactions flying around the network. They are both for the exact same payment, but they have different fingerprints and only one of them can be added to the public ledger.

Andreas Antonopoulos, chief security officer for the Blockchain.info Bitcoin wallet said: "The first one that is confirmed will be accounted for in the blockchain and will become the definitive record. The other will be dropped as a double spend attempt."

An error in the way Mt.Gox was auditing the blockchain to verify transactions allowed attackers to spoof non-successful transaction and get Mt.Gox to issue refunds.

This IS something that needs to be resolved in the protocol... but all Bitcoin users need to do now, to be safe, is don't issue transactions too rapidly. Allow ten minutes for a transaction to "take hold" in the network.

Dozens of rogue self-signed SSL certificates used to impersonate high-profile sites

- http://news.netcraft.com/archives/2014/02/12/fake-ssl-certificates-deployed-across-the-internet.html
- http://www.pcworld.com/article/2097781/dozens-of-rogue-selfsigned-ssl-certificates-used-to-impersonate-highprofile-sites.html
- Lack of CA checking is real!:
    - Researchers from Stanford University and The University of Texas at Austin found broken SSL certificate validation in Amazon's EC2 Java library, Amazon's and PayPal's merchant SDKs, integrated shopping carts such as osCommerce and ZenCart, and AdMob code used by mobile websites. A lack of certificate checks within the popular Steam gaming platform also allowed consumer PayPal payments to be undetectably intercepted for at least 3 months before eventually being fixed.

    - Online banking apps for mobile devices are tempting targets for man-in-the-middle attacks, as SSL certificate validation is far from trivial, and mobile applications often fall short of the standard of validation performed by web browsers. 40% of iOS-based banking apps tested by IO Active are vulnerable to such attacks because they fail to validate the authenticity of SSL certificates presented by the server. 41% of selected Android apps were found to be vulnerable in manual tests by Leibniz University of Hannover and Philipps University of Marburg in Germany.

Sci-Fi:

- Ender's Game was BETTER the 2nd time around.
- RoboCop FAR exceeded my (and Jenny's) expectations.
- "Transcendence" -- mid-April -- looks AWESOME!

SQRL:

- The UI Page is coming to life: https://www.grc.com/sqrl/operation.htm
- http://bit.ly/sqrlui