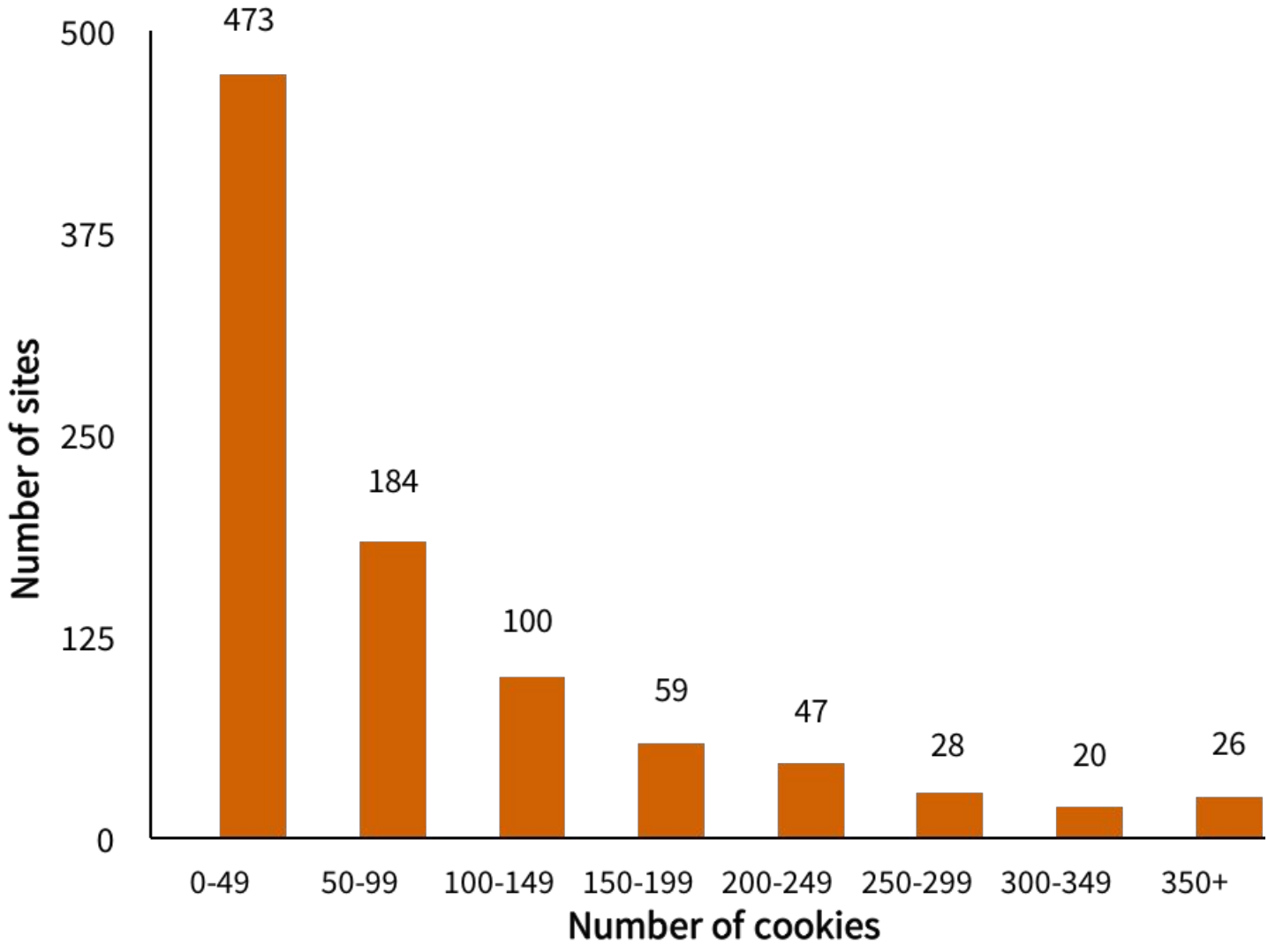
Security Now! #539 - 12-22-15

Q&A #226

This week on Security Now!

- The stunning Juniper Router Backdoor.
- Oracle gets smacked by the US Federal Trade Commission.
- What happens if you simply press backspace 28 times at a Linux password prompt?
- WhatsApp briefly banned in Brazil - what it means?
- Hillary's call for a Manhattan-style effort on encryption
- A recent audit provides an updated snapshot of the state of Web Privacy.
- Microsoft increases the GWX controversy.
- A bit of miscellany,
- A tip about managing "always on" DVR recorders,
- Questions and Answers from our passionately involved listeners.



Security News:

Juniper: IMPORTANT JUNIPER SECURITY ANNOUNCEMENT POSTED BY BOB WORRALL, SVP CHIEF INFORMATION OFFICER ON DECEMBER 17, 2015

- http://forums.juniper.net/t5/Security-Incident-Response/Important-Announcement-about-ScreenOS/ba-p/285554
- CVE-2015-7755: Juniper ScreenOS Authentication Backdoor
- Adam Langley's Weblog
  - https://www.imperialviolet.org/2015/12/19/juniper.html
- Researchers Solve Juniper Backdoor Mystery; Signs Point to NSA
  - http://www.wired.com/2015/12/researchers-solve-the-juniper-mystery-and-they-say-its-partially-the-nsas-fault/
- Matthew Green: On the Juniper backdoor
  http://blog.cryptographyengineering.com/
  You might have heard that a few days ago, Juniper Systems announced the discovery of "unauthorized code" in the ScreenOS software that underlies the NetScreen line of devices. As a result of this discovery, the company announced a pair of separate vulnerabilities, CVE-2015-7755 and CVE-2015-7756 and urged their customers to patch immediately.

  The first of these CVEs (#7755) was an authentication vulnerability, caused by a malicious hardcoded password in SSH and Telnet. Rapid7 has an excellent writeup of the issue.

  https://community.rapid7.com/community/infosec/blog/2015/12/20/cve-2015-7755-juniper-screenos-authentication-backdoor

  This is a pretty fantastic vulnerability, if you measure by the impact on security of NetScreen users. But on the technological awesomeness scale it only rates only about a two out of ten, maybe a step above 'hit the guy with a wrench'.

  The second vulnerability is a whole different animal. The advisory notes that CVE-7756 -- which is independent of the first issue -- "may allow a knowledgeable attacker who can monitor VPN traffic to decrypt that traffic." This is the kind of vulnerability that makes applied cryptographers cry tears of joy. It certainly did that for me:

  > I'm really invested in the idea that this Juniper encryption vulnerability is going to be amazing. Like, Flame-level amazing.
  > — Matthew Green (@matthew_d_green) December 18, 2015

- And while every reasonable person knows you can't just drop "passive decryption vulnerability" and expect the world to go on with its business, this is exactly what Juniper tried to do. Since they weren't talking about it, it fell to software experts to try to work out what was happening by looking carefully at firmware released by the company.

  Now I want to be clear that I was not one of those software experts. IDA [Interactive DisAssembler] scares the crap out of me. But I'm fortunate to know some of the right kind of people, like Steve Checkoway, who I was able to get on the job, mostly by encouraging

him to neglect his professional obligations. I also follow some talented folks on Twitter, like H.D. Moore and Ralf Philipp Weinmann. So I was fortunate enough to watch them work, and occasionally (I think?) chip in a helpful observation.

And yes, it was worth it. Because what Ralf and Steve et al. found is beyond belief. Ralf's excellent post provides all of the technical details, and you should honestly just stop reading now and go read that.

https://rpw.sh/blog/2015/12/21/the-backdoored-backdoor/

But since you're still here, the TL;DR is this:

  - For the past several years, it appears that Juniper NetScreen devices have incorporated a potentially backdoored random number generator, based on the NSA's Dual_EC_DRBG algorithm. At some point in 2012, the NetScreen code was further subverted by some unknown party, so that the very same backdoor could be used to eavesdrop on NetScreen connections. While this alteration was not authorized by Juniper, it's important to note that the attacker made no major code changes to the encryption mechanism -- they only changed parameters. This means that the systems were potentially vulnerable to other parties, even beforehand. Worse, the nature of this vulnerability is particularly insidious and generally messed up.

- Someone changed "Q"

- P and Q are supposed to be randomly arrived at values without any known relationship.

- But back in 2007, researchers discovered that if there was a relationship such that in a finite field Q=P*e modulus the field size (where the 'e' relationship was secret but known to an attacker) then after sampling a very small bit of Dual_EC_DRBG output, the internal state of the PRNG could be determined ... and all future random numbers would be known.

- But in the Juniper code, the Dual_EC_DRBG is only used to provide the seed to a high-quality TripleDES PRNG. So it seemed that, super suspicious as the changed "Q" parameter was, there wasn't any obvious way for an attacker to use it.

- Then they discovered that an ultra-subtle "bug" in the code -- where a buffer pointer is not reset to zero -- prevents the high-quality post-Dual_EC_DRBG PRNG from being used... thus making the Dual_EC_DRBG's values available to anyone monitoring the device.

- And... IF that person also knew the secret relationship between P and Q... they could then PASSIVELY DECRYPT all of that device's traffic.

- No logs, no evidence. Just capture the traffic and decrypt it.
- The MASSIVE question is... WHO DID THIS??

Oracle gets smacked by the FTC over Java SE security

- https://www.washingtonpost.com/news/the-switch/wp/2015/12/21/nearly-a-billion-pcs-run-this-notoriously-insecure-software-now-oracle-has-to-clean-it-up/
- Oracle Ordered to Publicly Admit Misleading Java Security Updates
  - http://thehackernews.com/2015/12/java-insecure-hacking.html
- Engadget: Oracle settles charges that it misled you on Java security
  - http://www.engadget.com/2015/12/21/oracle-settles-with-ftc-over-java/
- Oracle has to not only notify you about its security risks, but help you uninstall vulnerable Java copies.
- FTC: Oracle Agrees to Settle FTC Charges It Deceived Consumers About Java Software Updates Company Will Be Required to Notify Consumers of Risk, Provide Tools to Uninstall Insecure Older Versions
  - https://www.ftc.gov/news-events/press-releases/2015/12/oracle-agrees-settle-ftc-charges-it-deceived-consumers-about-java
- Oracle has agreed to settle Federal Trade Commission charges that it deceived consumers about the security provided by updates to its Java Platform, Standard Edition software (Java SE), which is installed on more than 850 million personal computers. Under the terms of a proposed consent order, Oracle will be required to give consumers the ability to easily uninstall insecure, older versions of Java SE.

  Jessica Rich, director of the FTC's Bureau of Consumer Protection: "When a company's software is on hundreds of millions of computers, it is vital that its statements are true and its security updates actually provide security for the software. The FTC's settlement requires Oracle to give Java users the tools and information they need to protect their computers."

  Oracle's Java SE provides support for a vast array of features consumers use when browsing the web, including browser-based calculators, online gaming, chatrooms, and 3D image viewing.

  According to the FTC's complaint, since acquiring Java in 2010, Oracle was aware of significant security issues affecting older versions of Java SE. The security issues allowed hackers' to craft malware that could allow access to consumers' usernames and passwords for financial accounts, and allow hackers to acquire other sensitive personal information through phishing attacks.

  In its complaint, the FTC alleges that Oracle promised consumers that by installing its updates to Java SE both the updates and the consumer's system would be "safe and secure" with the "latest… security updates." During the update process, however, Oracle failed to inform consumers that the Java SE update automatically removed only the most recent prior version of the software, and did not remove any other earlier versions of Java SE that might be installed on their computer, and did not uninstall any versions released prior to Java SE version 6 update 10. As a result, after updating Java SE, consumers could still have additional older, insecure versions of the software on their computers that were vulnerable to being hacked.

  In 2011, according to the FTC's complaint, Oracle was aware of the insufficiency of its update process. Internal documents stated that the "Java update mechanism is not

aggressive enough or simply not working," and that a large number of hacking incidents were targeting prior versions of Java SE's software still installed on consumers' computers.

Under the terms of the proposed consent order, Oracle will be required to notify consumers during the Java SE update process if they have outdated versions of the software on their computer, notify them of the risk of having the older software, and give them the option to uninstall it. In addition, the company will be required to provide broad notice to consumers via social media and their website about the settlement and how consumers can remove older versions of the software.

The consent order also will prohibit the company from making any further deceptive statements to consumers about the privacy or security of its software and the ability to uninstall older versions of any software Oracle provides.

Break into a Linux computer just by pressing backspace 28 times!

- http://thehackernews.com/2015/12/hack-linux-grub-password.html
- Ubuntu, Red Hat and Debian have all released emergency patches.
- Grub2 (Grand Unified Bootloader) used by most Linux systems to boot the OS.
- Just hit the backspace key 28 times at the Grub username prompt during power-up. This will open a "Grub rescue shell" under Grub2 versions 1.98 to version 2.02.
- This rescue shell allows unauthenticated access to a computer and the ability to load another environment.
- Researchers have verified that from this shell, an attacker could gain access to all the data on your computer, and can misuse it to steal or delete all the data, or install persistent malware or rootkit.
- The source of the vulnerability is an integer underflow fault that was introduced with single commit in Grub version 1.98 (December 2009) in the grub_password_get() function.

WhatsApp Banned for 48 Hours (and then not) in Brazil

- http://www.pcmag.com/article2/0,2817,2496766,00.asp
- The move comes after WhatsApp failed to respond to a court order in a criminal case.
- Then: A Brazilian judge on Thursday lifted the ban, overturning the lower court's decision, according to Reuters.
- Brazil court lifts suspension of Facebook's WhatsApp service
    - http://www.reuters.com/article/us-brazil-whatsapp-ban-idUSKBN0U000G20151217
- [Paraphrased]
  After about 12 hours, a Brazilian appellate judge on Thursday ordered the lifting of a 48-hour suspension of the services in Brazil of Facebook Inc's WhatsApp phone-messaging application, overturning an order from a lower court.

  The interruption of WhatsApp's text message and Internet telephone service caused outrage in Latin America's largest country, where the company estimates it has 100 million personal users, and led to angry exchanges on the floor of Congress.

WhatsApp is installed on 92.5% of Android devices in Brazil, making it the most installed app in the country, according to SimilarWeb, an internet intelligence and marketing company.

Rival messaging system Telegram said on Twitter that it received 1 million downloads in Brazil in one day due to the outage. Telegram was installed on 2.35 percent of android devices before the blackout and Facebook Messenger on 74 percent.

A judge in an industrial suburb of Sao Paulo, had ordered the suspension of WhatsApp's services from midnight on Wednesday (0200 GMT Thursday). The order was made after WhatsApp, despite a fine, failed to comply with two judicial rulings to share information in a criminal case.

Judge Xavier de Souza, who overturned the lower court order said: "Considering the constitutional principles, it does not look reasonable that millions of users be affected as a result of the company's inertia to provide information." However, he then recommended that a higher fine be imposed on WhatsApp.

The incident highlighted growing international tensions between technology companies' privacy concerns and national authorities' efforts to use social media to recover information on possible criminal activities.

Mark Zuckerberg (responding from his nursery) said: "Until today, Brazil has been an ally in creating an open Internet. I am stunned that our efforts to protect people's data would result in such an extreme decision by a single judge to punish every person in Brazil who uses WhatsApp."

According to Band News TV, the criminal case involves a drug trafficker linked to one of Sao Paulo's most dangerous criminal gangs. The trafficker allegedly used WhatsApp services while committing crimes, and the court wants access to his communications with others.

WhatsApp said it was unable, not unwilling, to comply.

ArsTechnia: Hillary Clinton wants "Manhattan-like project" to break encryption

- http://arstechnica.com/tech-policy/2015/12/hillary-clinton-wants-manhattan-like-project-to-break-encryption/
- "Presidential candidate Hillary Clinton has called for a "Manhattan-like project" to help law enforcement break into encrypted communications."
- No... she didn't.
- She called for the tech community and law enforcement to work together to solve this apparently "really hard" problem.
- Her reference to a Manhattan-like project was her assumption that the problem is just big and difficult.. but with sufficient resources CAN be solved.

Web Privacy Census

- http://techscience.org/a/2015121502/

Description	Date	Type	Sites Crawled	Total HTTP Cookies	First-Party HTTP Cookies	Third-Party HTTP Cookies	Sites Using Flash Cookies	Sites Using HTML5 Local Storage
Top 100 Sites	2015-07-01	shallow	100	6,280	1,091 (17%)	5,189 (83%)	5 (5%)	63 (63%)
Top 100 Sites	2015-07-01	deep	100	1,2857	1,265 (10%)	11,592 (90%)	10 (10%)	76 (76%)
Top 1,000 Sites	2015-07-01	shallow	1,000	80,821	10,374 (13%)	70,447 (87%)	39 (4%)	613 (61%)
Top 1,000 Sites	2015-07-01	deep	1,000	134,769	10,871 (8%)	123,898 (92%)	62 (6%)	649 (65%)
Top 25,000 Sites	2015-07-01	shallow	25,000	1,065,076	135,767 (13%)	929,309 (87%)	585 (2%)	8,688 (35%)

New GWX ploy: "Upgrade Now" or "Upgrade Tonight"

- Woody Leonard / Woody on Windows InfoWorld Column:
  Microsoft narrows Win10 upgrade options to 'Upgrade now' or 'Upgrade tonight'
  Microsoft's nagging 'Get Windows 10' campaign has hit a confusing new low -- and user backlash is vocal
- http://www.infoworld.com/article/3015238/microsoft-windows/microsoft-narrows-win10-upgrade-options-to-upgrade-now-or-upgrade-tonight.html
- It's hard to imagine any marketing campaign worse than Microsoft's ongoing "Get Windows 10" debacle. Microsoft is pushing hard for Windows 7 and 8.1 customers to upgrade to Windows 10, and the backlash from users has been vocal and very negative.

  Paying Windows 7 and 8.1 customers have been subjected to:

  - Surreptitious installation of a potentially unwanted program, GWX, starting way back in April
  - Incessant nagging by a balloon notification in the system tray that "Your upgrade is ready"
  - Forced download of 3GB to 5GB of unwanted installation files
  - "Accidental" automatic launching of the upgrade program

- Last week PC World's Brad Chacos detailed the evolution of the nagging GWX balloon notification into a full-fledged (and nearly full-screen) Get Windows 10 window with two options: "Upgrade now" and "Start download, upgrade later." Per Chacos:

  - To be fair, you can still simply close the window using the X in the upper-right corner, and if you click through the itty-bitty inconspicuous chevron on the right-edge of the window there may be a "Nope" prompt somewhere further down the line. (I closed the prompt before exploring the auxiliary pages.) But having the

only two large, clearly actionable options on a pop-up page both lead to a Windows 10 download feels inherently icky—like Microsoft's trying to trick less-savvy computer users into downloading the operating system with tactics often used by spammers and malicious websites.

Miscellany:

Star Wars

- Star Wars breaks all time 1st weekend sales record: $248 Million.
- (And about twice that worldwide.)

Homeland - Season 3 finishes, Will there be a season 6?

- It appears so!
- http://tvline.com/2015/12/09/homeland-renewed-season-6-showtime/
- Showtime on Wednesday officially renewed the Sunday drama for a sixth season.

SpinRite

SpinRite and Always-Recording devices

- https://jervis.ws/spinrite-and-the-humax-dtr-t1000-youview-hd-digital-tv-recorder/
- The trouble.
- Continuously recording for pause
- How to safely shutdown