Security Now! #495 - 02-17-15

HTTP/2

This week on Security Now!

- Google compromises a bit on its "Project Zero" idealogy,
- Hackers perpetrate a massive coordinated global banking heist,
- Kaspersky Lab reveals the equivalent of "Bad USB" for hard drives,
- "Credit Freezing" offers strong identity theft protection,
- ...and... a close look at the forthcoming HTTP/2 standard.

Why “Blacklisting” Fails

Image of the Week, thanks to Simon Zerafa

Security News

Google's Project Zero adding 14-day grace period...

- via: Matthew Leidholm @MattLeidholm
- @SGgrc Google's Project Zero adding 14-day grace period if vendor schedules patch's release just after 90 days googleprojectzero.blogspot.com/2015/02/feedba…
- http://googleprojectzero.blogspot.com/2015/02/feedback-and-data-driven-updates-to.html
- Google's blob post takes a somewhat defensive tone, noting several other day-count limited disclosure policies.
- Uses Adobe as an example of their system working:
  - To see how things are going, we crunched some data on Project Zero’s disclosures to date. For example, the Adobe Flash team probably has the largest install base and number of build combinations of any of the products we’ve researched so far. To date, they have fixed 37 Project Zero vulnerabilities (or 100%) within the 90-day deadline.

    More generally, of 154 Project Zero bugs fixed so far, 85% were fixed within 90 days. Restrict this to the 73 issues filed and fixed after Oct 1st, 2014 [presumably meaning after the system was up and running and more well known], and 95% were fixed within 90 days. Furthermore, recent well-discussed deadline misses [Windows and OS X] were typically fixed very quickly after 90 days. Looking ahead, we’re not going to have any deadline misses for at least the rest of February.
- Finally:
  <quote> Deadlines appear to be working to improve patch times and end user security -- especially when enforced consistently.

  We’ve studied the above data and taken on board some great debate and external feedback around some of the corner cases for disclosure deadlines. We have improved the policy in the following ways:

- **Weekends and holidays.**
  - If a deadline is due to expire on a weekend or US public holiday, the deadline will be moved to the next normal work day.

- **Grace period.**
  - We now have a 14-day grace period. If a 90-day deadline will expire but a vendor lets us know before the deadline that a patch is scheduled for release on a specific day within 14 days following the deadline, the public disclosure will be delayed until the availability of the patch. Public disclosure of an unpatched issue now only occurs if a deadline will be significantly missed (2 weeks+).

- **Assignment of CVEs.**
  - CVEs are an industry standard for uniquely identifying vulnerabilities. To avoid confusion, it’s important that the first public mention of a vulnerability should include a CVE. For vulnerabilities that go past deadline, we’ll ensure that a CVE has been pre-assigned.

Global Bank Heist

- (A lot of news is flowing due to the Kaspersky Security Analyst Summit, 2015 going on right now in Cancun, Mexico.)
- http://usa.kaspersky.com/about-us/press-center/press-releases/great-bank-robbery-carbanak-cybergang-steals-1-billion-100-fina
- "Carbanak" Cybercrime group -- a new type of Advanced Persistent Threat.
- Operating since 2013, silently attacking at least 100 banks, e-Payment systems, and other financial institutions in 30 countries. The group remains active today.
- Each raid was limited to $10 million and required two to four months to setup.
- Intruders in the bank thefts were enormously patient.
- Placed surveillance software in the computers of system administrators and watching their moves for months.
- Watched, studied and learned a victim bank's normal operating procedures, then used those to siphon money.
- Kaspersky has accumulated evidence of $300 Million, but expects triple that.
- Most banking targets were in Russia, but many in Japan, the USA, and Europe.
- Banks have remained silent.
- Funds transfer-to target banks were J.P.Morgan Chase in the US and Agricultural Bank of China.
- Some money was exfiltrated in cash from ATMs which would dispense on schedule.
  - One Kaspersky banking client lost $7.3 million through ATM cash transfers alone.
- Largest transfers were by wire:
  - Tweak an existing account with $1,000 to show a balance of $10,000,
  - then transfer $9,000 from that account offshore... restoring the account's balance to $1,000.
  - One client lost $10 million this way.
- As Kaspersky Lab described it (in their press release, yesterday, on the first day of their Security Analyst Summit in Cancun)
  - The cybercriminals began by gaining entry into an employee’s computer through spear phishing, infecting the victim with the Carbanak malware. They were then able to jump into the internal network and track down administrators’ computers for video surveillance. This allowed them to see and record everything that happened on the screens of staff who serviced the cash transfer systems. In this way the cyber criminals got to know every last detail of the bank clerks’ work and were able to mimic staff activity in order to transfer money and cash out.

Kaspersky reveals NSA hiding spyware on Hard Drives:

- http://bit.ly/bad-hdd
- https://securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf
- Reuters -- A good piece which explores this further:
- http://www.reuters.com/article/2015/02/17/us-usa-cyberspying-idUSKBN0LK1QV20150217
- Kaspersky calls them "The Equation group."

- They are affiliated with groups that generated Stuxnet and Regin, and they were using the unknown 0-day vulnerabilities used by Stuxnet and Regin BEFORE those projects used them.
- <quote>
  Perhaps the most powerful tool in the Equation group's arsenal is a mysterious module known only by a cryptic name: "nls_933w.dll". It allows them to reprogram the hard drive firmware of over a dozen different hard drive brands, including Seagate, Western Digital, Toshiba, Maxtor and IBM. This is an astonishing technical accomplishment and is testament to the group's abilities.

- Kaspersky writes:
  The main function to reflash the HDD firmware receives an external payload, which can be compressed by LZMA. The disk is targeted by a specific serial number and reprogrammed by a series of ATA commands. For example, in the case of Seagate drives, we see a chain of commands: "FLUSH CACHE" (E7), "DOWNLOAD MICROCODE" (92), "IDENTIFY DEVICE" (EC), "WRITE LOG EXT" (3F). Depending on the reflashing request, there might be some unclear data manipulations written to the drive using "WRITE LOG EXT" (3F). For WD drives, there is a sub-routine searching for ARM NOP opcodes in read data, and then used further in following writes. Overall, the plug-in uses a lot of undocumented, vendor-specific ATA commands, for the drives mentioned above as well as all the others.

- The EQUATION group's HDD firmware reprogramming module is extremely rare. During our research, we've only identified a few victims who were targeted by this module. This indicates that it is probably only kept for the most valuable victims or for some very unusual circumstances.

- Persistence, Invisibility, Local Caching
- Extreme, hardware-locked persistence survives disk formatting and OS reinstallation.
  - If the malware gets into the firmware, it is available to “resurrect” itself forever. It may prevent the deletion of a certain disk sector or substitute it with a malicious one during system boot.

- Once the hard drive gets infected with this malicious payload, it is impossible to scan its firmware.
  - There are functions to write into the hardware firmware area, but there are no functions to read it back. This means that malware scanners are effectively blind.

- An invisible, persistent, non-volatile area hidden inside the hard drive.
  - Can be used to cache exfiltrated information which can be later retrieved by the attackers. Can save transiently present decryption keys, etc.

- **F-Secure reminds us about "IRATEMONK"** from the December 29th, 2013 Der Spiegel article about the NSA's catalog of exploit technologies:
- https://www.f-secure.com/weblog/archives/00002791.html
- <quote> (TS//SI/REL) IRATEMONK provides software application persistence on desktop and laptop computers by implanting the hard drive firmware to gain execution through Master Boot Record (MBR) substitution.

- <quote> This technique supports systems withoutt RAAID hardware that boot from a variety of Western Digital, Seagate, Maxtor, and Samsung hard drives. The supported file systems are FAT, NTFS, EXT3 and UFS.
- <quote> Through remote access or interdiction, UNITEDDRAKE or STRAIGHTBLAZE are used in conjunction with SLICKERVICAR to upload the hard drive firmware onto the target machine to implant IRATEMONK and its payload (the implant installer). Once implanted, IRATEMONK's frequency of execution (dropping the payload) is configurable and will occur when the target machine powers on.

- Hacking a hard drive's internals: (Via Simon Zerafa, thanks!) http://spritesmods.com/?art=hddhack

"Credit Freezing" to thwart identity theft

- http://bit.ly/freezecredit
- "A credit freeze will stop criminals from opening new credit in your name"
- What is identity theft?
- Credit Freeze cost ranges from $3 to $10. (CA was $10)
- Equifax, Experian, TransUnion

Sci-Fi Update

- Finished with Expanse Book #2 -- SO FUN!
- "Caliban's War"
- http://www.syfy.com/theexpanse/videos/the-expanse-trailer
- Protomolecule / Solar System politics.

SpinRite

Igor Koveshnikov in New Jersey
(He'd put an SSD in his boss's machine, it went bad, SpinRite fixed it.)

Question: it’s related to my testimonial. As far as I understand SSD completely hides its internal structure behind wear leveling and optimization in firmware, and represent the drive externally as a standard mechanical drive. When SpinRite runs on level 2 and higher, it reads a sector and then writes it -- supposedly to the same sector. But SSD is using wear leveling and writes data to whatever its algorithm decides are the most appropriate cells in memory, and may not be the same that the data was read from. Is there any way to get closer to the hardware of SSD and SSHD (hybrid) or will it always be a “black box”? Will it be addressed in the new version? Right now, according to my own and many other users' experiences, we know that SpinRite repairs SSDs just like hard drives, but I think we can only speculate on how. If you ever come across more info on internal “mechanics” of SSDs, please share it with us, preferably on SN.
Shout out: to my wife, she’s a software security specialist and listens to every episode of SN.

HTTP/2

http://tools.ietf.org/pdf/draft-ietf-httpbis-http2-17.pdf
HTTP/2, Draft #17, February 11th, 2015

What's wrong with what we already have?

- Utterly insane pages.
- Very simple, textual, receipt/request model
    - (client asks, server doesn't send)
- Each request is stand alone, entirely stateless, and doesn't presume any knowledge or context of anything previous.
- TCP has high per-connection overhead and a slow-start rate control.
- TLS has high per-connection crypto negotiation.
- In order to overcome HTTP/1.x's limitations, multiple connections.

HTTP/2 fixes all that.

- Identifying an HTTP/2 connection
    - There CAN be some in-band negotiation, especially for non-TLS
    - TLS v1.2 defines a special "pseudo cipher suite" to hoist the version during TLS negotiation.

- Frames:
    - 9-byte frame header:
        - 24-bit length (only 14 bits okay without other side's permission)
            - (Length excludes the 9 bytes header)
        - 8-bit frame type
        - 8 bits of frame type specific flags
        - 32-bit stream ID (but the high bit is always 0)
    - <<variable length (specified length) payload>>

- Frames
    - Dividing the single connection flow into numbered frames:

- Streams
    - Priorities can be assigned by the requestor
    - Inter-stream dependencies can be assigned.
    - Allocate limited resources to the identified stream in preference to the dependent stream.

- HTTP Headers & Compression
    - How LZ (Lempel-Ziv) operates. (PKZIP, GZIP, LZW, LZA, etc.)
    - A single compression context for the connection.

- "Speculative Push"