Security Now! #476 - 10-07-14

Q&A #198

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!

- The largest ever breach: JP Morgan Chase.
- Yahoo!'s servers hit by ShellShock.
- BadUSB exploit code posted to Github.
- Bugzilla has a bug!... Does it report itself?
- Some Sci-Fi miscellany, I answer an interesting SpinRite question, and our Q&A!

Security News:

JP Morgan Chase Breach

- (News of last Thursday, Oct. 2nd)
- 76 million households & 7 million small businesses (thus, among the largest ever).
- Disclosed in a securities filing on Thursday.
- Attack began in June, not discovered until July.
- On the condition of anonymity, people with knowledge of the investigation revealed that attackers appeared to have obtained a list of the software being used on JPMorgan's computers and then cross-checked that with all known vulnerabilities in each program and web application.
- Overseas attackers gained access to:
    - Names, addresses, phone numbers, and eMail addresses of JPMorgan account holders.
- No evidence that account information, passwords, or SS #'s had been taken.
- And no evidence of fraud involving the use of the exfiltrated information.
- However... tidbits of what we know:
    - By the time the bank's security team discovered the breach in late July, attackers had obtained the highest level of administrative privilege to dozens of the bank's computer servers.
    - They penetrated deeply into the bank's computer systems, reaching more than 90 servers.
    - However, there is no evidence that the attackers stole even a penny from the customer accounts to which they had access.
    - And... It is still unclear how, exactly, they managed to gain such complete access.

The next day: NYTimes reports that **nine** other large financial institutions were also affected, though no more details were forthcoming.

In breathless news: "Yahoo Servers Were Owned By Bash Bug Hackers"

- "Yahoo Servers Were Owned By Bash Bug Hackers"
- http://www.forbes.com/sites/thomasbrewster/2014/10/06/yahoo-hacked-by-bash-bug-attackers/
- Shellshock rising: Yahoo's servers reportedly compromised by devastating bug
- http://pando.com/2014/10/06/shellshock-rising-yahoos-servers-reportedly-compromised-by-devastating-bug/
- Yahoo! CISO Alex Stamos clarified what happened over the weekend. He explained that although the attackers were looking to exploit Bash, at Yahoo they happened to take advantage of a separate bug, possibly without knowing it...

  "It turns out that the servers were in fact not affected by Shellshock. Three of our Sports API servers had malicious code executed on them this weekend by attackers looking for vulnerable Shellshock servers. These attackers had mutated their exploit… This mutation happened to exactly fit a command injection bug in a monitoring script our Sports team was using at that moment to parse and debug their web logs. The affected API servers are used to provide live game streaming data to our Sports front-end and do not store user data. At this time we have found no evidence that the attackers compromised any other machines or that any user data was affected. This flaw was specific to a small number of machines and has been fixed."

BadUSB returns: (Different) Hackers publish code that could infect millions of USB devices

- https://github.com/adamcaudill/Psychson

- 1st: July, BlackHat, Karsten Nohl demonstrates but does not release "BadUSB" discovery.
  2nd: At the DerbyCon hacker conference last week, Adam Caudill & Brandon Wilson demonstrated that they had followed in Karsten's footsteps... but they put their full exploit kit up on Github.
  Adam said to the DerbyCon audience: "The belief we have is that all of this should be public. It shouldn't be held back. So we're releasing everything we've got. This was largely inspired by the fact that [SR Labs] didn't release their material. If you're going to prove there's a flaw, you need to release the material so people can defend against it."

- Some Phison-based USB drives.
  - Phison is one of the top Taiwanese-based USB memory suppliers.

- 8051-based microcontroller
  - .NET 4.0 with Visual Studio 2012 Express.
  - SDCC (Small Device C Compiler)
    - Open source C compiler for the 8051
- Known vulnerable devices:
  - Patriot 8GB Supersonic Xpress
  - Patriot Stellar 64 Gb Phison
  - Kingston DataTraveler 3.0 T111 8GB
  - Silicon power marvel M60 64GB
  - Toshiba TransMemory-MX™ Black 16 GB

- **Adam's own Q&A:**
- What we released:
    - Patch to demonstrate the feasibility of creating a hidden partition on a USB thumb drive.
    - Password Bypass modifies/defeats the device's password protection mechanism.
        - (But the patch must be applied BEFORE the user sets their password, so it doesn't really defeat any meaningful security.)

    - The patches were carefully selected to make the point, while not endangering users.
    - Custom Firmware for converting the device into a HID (Human Interface Device) keyboard.
    - The Toolset to help in playing with these things.

- What was NOT released:

    - **Self Replication** - <quote> There's no self replication code anywhere, while it's possible that it could be done, and we've talked about how to do it - it won't be released.

      I am confident that we (Brandon and I) could build a system that would infect PCs, then infect a significant percentage of thumb drives, and then infect other PCs - but, and this is a big but - what we released doesn't make that easier in any significant way.

      Your average script kiddy will never be able to do it; there's only a small number of people that would be able to do the work needed to be able to pull it off - those people could already do it before we released what we did.

      The threat of this happening is the same as it has always been.

    - **Malware** - There's nothing malicious about what we've released here. While we did release a patch to modify the password protection feature - that's all it does. It doesn't modify data, infect computers with anything, or anything of that nature.

      It changes the way a feature works. That's it. This is a change that anyone with the required skills could have made - by making it public, we are raising awareness that users shouldn't blindly trust.

    - **The end of USB as we know it** - Nothing, nothing, that we've released has suddenly made new attacks possible. The USB specification allows composite devices to do unexpected things. USB devices (thumb drives or otherwise) that allow anyone to update the firmware without any checks, means that anything can potentially be reprogrammed to change functionality or become malicious.

      All of these things have been true long before we released the first line of code. Anyone that believes otherwise doesn't understand the technology.

- **An unfixable issue that will end the world** - While there isn't quick fix for this, things can be improved quite a bit. We released simple code, that proves the issue, draws attention to the fact that users need to be more careful, while being careful to not cause more harm than good in the process.

  This isn't earth shattering. Anyone that thinks that it is, should probably give up and go live in a cave.

Bugzilla Zero-Day Exposes Zero-Day Bugs

- http://krebsonsecurity.com/2014/10/bugzilla-zero-day-exposes-zero-day-bugs/
- Upon account creation, eMail addresses were not being verified.
- Non-default settings allowed privileges to be tied to eMail account domain names.
- Whoops!
- So: IF a Bugzilla admin chose to allow domain name based privileges, THEN anyone could obtain access to potentially sensitive internal privately reported and pending-repair security vulnerabilities.

This Week in SciFi:

"Edge of Tomorrow"

- IMDB: 8/10, Rotten Tomatoes: 90% (Audience Score: 91%)
- Last time: Oblivion -- great!

Interstellar Trailer

- " With our time on Earth coming to an end, a team of explorers undertakes the most important mission in human history; traveling beyond this galaxy to discover whether mankind has a future among the stars. " (Matthew McConaughey, Anne Hathaway, Michael Caine, Casey Affleck)

Miscellany:

- Homeland Season #4.

SpinRite:

Martin in Frankfurt, Germany, wonders how much use he might be able to get out of a troubled drive?

Hello Steve,

I have a question about how safe it is to still use a drive after it was SpinRite'ed (yay, official new word since the last Security Now podcast!) and SpinRite has found sectors that are not recoverable.

In such an instance, does SpinRite tell the drive to map out those bad sectors so they will never be used again? Is it therefore safe to still use the drive and the remaining good portion? Or should one consider not using the drive at all any more since it shows rather severe damage?

I guess it all depends on the overall age and usage of the drive and how important the data you want to put on the drive is to you. But just from a purely technical point of view, would SpinRite move those bad apples out of the way for you?

As always, thank you for your great wisdom and advice!

Martin