Security Now! #485 - 12-09-14

Expensive Lessons

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!

- "De-TOR" Deep Dive coming soon!... bumped by Sony!
- "POODLE" bites us again!
- A longstanding APT jumps platforms… to Linux!
- VERY worrisome statements from a prominent US District Court Judge Posner.
- Miscellany, answering a SpinRite question, and...
- Expensive Lessons: TARGET and SONY

Jenny's and her daughter's two Neuf sisters

Security News:

Poodle Bites (again!)

- Links:
  - https://www.imperialviolet.org/2014/12/08/poodleagain.html
  - http://arstechnica.com/security/2014/12/meaner-poodle-bug-that-bypasses-tls-crypto-bites-10-percent-of-websites/
- ssllabs.com
  - https://community.qualys.com/blogs/securitylabs/2014/12/08/ssl-labs-end-of-year-2014-updates
  - http://blog.ivanristic.com/2014/12/poodle-bites-tls.html
- POODLE was about playing with the padding bytes required for block ciphers.
  - (Block ciphers require an exact multiple of bytes. So some padding is required.)
- Unlike the TLS specs, SSL never specified what the padding bytes were, and...
- When sending, SSLv3 makes the mistake of authenticating THEN encrypting.
- Therefore, when receiving the reverse sequence is decryption THEN authentication. This allows probing of the encrypted contents.
- Even though TLS REQUIRES specific padding bytes, thus preventing POODLE... it turns out that many TLS stacks DON'T BOTHER CHECKING that the padding bytes are conforming... thus making them ALSO vulnerable to POODLE.
- It appears that about 10% of websites are vulnerable to a newer variant of the POODLE attack which works against TLS... even the latest version 1.2.
- F5 and A10 load balancing SSL/TLS accelerator appliances.

TURLA - An APT (Advanced Persistent Threat) targeting Linux

- AKA: Uroburos or Snake
- Has been spotted:
  - 32 times in the Ukraine since 2010
  - 11 times in Lithuania
  - 4 times in the UK
  - A handful of times altogether from the US, Belgium, Georgia, Romania, Hungary and Italy.
- These are only the samples that have been discovered.
- Allows reliable inference that SNAKE has been aimed at Western and Western-aligned countries pretty much exclusively.

- Based upon code timestamps the timezone appears to be UTC+4 and the coders work Monday through Friday, taking weekends off.

- Kaspersky Lab and Symantec
- All previous TURLA samples were 32 or 64 bit WINDOWS executables.
- Used two 0-day exploits:
  - CVE-2013-5065 - Privilege escalation vulnerability in Windows XP and Windows 2003
  - CVE-2013-3346 - Arbitrary code-execution vulnerability in Adobe Reader
  - And also other patched vulnerabilities.

- Multiple backdoors are often run in tandem and used to "rescue" each other if either is discovered.
- Infection Vectors:
    - Spearphishing e-mails with Adobe PDF exploits (CVE-2013-3346 + CVE-2013-5065)
    - Social engineering to trick the user into running malware installers with ".SCR" extension, sometimes packed with RAR
    - Watering hole attacks using Java exploits (CVE-2012-1723), Flash exploits (unknown) or Internet Explorer 6,7,8 exploits (unknown)
    - Watering hole attacks that rely on social engineering to trick the user into running fake "Flash Player" malware installers
    - Attackers run a vast network of watering holes to precisely target visitors.

- Linux Offshoot:
    - Based upon a much older open-source Linux malware: cd00r (circa 2000).
    - Gives TURLA a wider reach since Linux is becoming increasingly popular and prevalent.
    - Large (800 KB), statically linked compiled C/C++ ELF executable with symbols stripped, includes:
        - GNU v2.3.2 C Library
        - OpenSSL v0.9.6 (somewhat old)
        - Libpcap - network capture library

    - Does NOT REQUIRE elevated privileges to run. No 'root' needed.
    - Won't show up in Netstat and maintains stealth without requiring elevated privilege.
    - A regular user with limited privileges can launch it inadvertently and it can intercept incoming packets and run incoming commands on the system.
    - Operation:
        - Uses PCAP to monitor incoming traffic with a raw socket.
        - If specific header bytes in incoming TCP or UDP packets "Magic Cookies" match, it opens a regular communications socket, connects to the IP address of the incoming magic packets, and drops into an endless loop ready to receive remote commands.
    - Appears to have been glued together from publicly available sources with specific added functions.

Judge Richard Posner - 7th Circuit Court

- http://boingboing.net/2014/12/08/judge-posner-it-should-be-ill.html
- "It should be illegal to make phones the government can't search."
- Speaking at a Georgetown law cybercrime conference:
- <quotes>
- "If the NSA wants to vacuum all the trillions of bits of information that are crawling through the electronic worldwide networks, I think that’s fine."
- Posner went on to say that privacy is "mainly about trying to improve your social and business opportunities by concealing the sorts of bad activities that would cause other people not to want to deal with you."

- On the idea of default full-disk encryption, he added "I'm shocked at the thought that a company would be permitted to manufacture an electronic product that the government would not be able to search."
- Cory Doctorow Writes:
    - <quote> "Posner conflates secrecy with privacy, another nonsense. Your parents did something un-secret to make you, but I'm willing to bet that Posner doesn't want his own non-secret, baby-making activity to be recorded and viewed by strangers."

Miscellany:

OddWorld:

"New n' Tasty"

iOS v8 Collapse:

- Add-on keyboard seem to hae the biggest problems.
- But not only that

Jenny and Bark Box:

- I just have to tell you. That dog box from your sponsor. OMG. I always thought that dog toys and treats are such a huge waste of money, but there was dog magic packed into that box. Every toy was played with--special treats inside!--until it was demolished and the food! I just gave them the box of dog stew, if you can believe that. I let them sniff it first and they sat there whimpering with impatience until I managed to set the bowls down. It disappeared in a flash.

- They ALL thank you. It was really fun.

- I sent you a photo of Paris and Beluga that you might use on your podcast when you share our reactions, which is all true, btw. I was impressed by that box, and I am not easily impressed, especially by anything dog. But our puppies are crazily photogenic, and Jaime just caught this moment, because Newfs, weirdly, often cross their front paws.

SpinRite:

Markus Sommer
Location: Germany
Subject: SpinRite & Full disk encryption
Date: 31 Jan 2012 10:06:52
:
Dear Steve,

I've been a "Security now"-listener for about 6 months now but I never bought a copy of SpinRite since I thought it to be a pure recovery-tool. However you recently mentioned that it is in fact a preventive maintenance tool, so I was thinking about getting a copy.

But there is a problem: due to privacy concerns I'm using full disk encryption (TrueCrypt) on all of my harddrives. Since this will effectively prevent SpinRite from seeing the datastructure on the hdd, I assume that it will not work on my harddrives.

Will I need to always decrypt the hdd, then run spinrite on it and then reencrypt it again or is there a way to work around this annoyance? (or might there be one in the next version of SpinRite, which you mentioned will be coming in the nearer future)

Love the podcast and I'm already waiting for the next part of "How the Internet works",

Markus

Expensive Lessons: Target & Sony

Target:

- At least 40 Million Target customer credit cards were compromised and as many as 110 million people may have had personal information, such as email addresses and phone numbers, stolen.
- Landslide of lawsuits were filed against Target, and they were consolidated into just two: One by consumers and one by banks.
- Target's lawyer argued that the company had no obligation to the banks because a third-party firm handles all credit and debit card payments... and asked that the suit be dismissed.
- A St. Paul Minnesota judge ruled that a lawsuit against Target over last year's breach could proceed because the retailer 'played a key role in allowing the harm to occur.'
- US District court judge Paul Magnuson wrote in a 16-page ruling: "Imposing a duty on Target in this case will aid Minnesota's policy of punishing companies that do not secure consumers' credit and debit card information. Although the third-party hackers' activities caused harm, Target played a key role in allowing the harm to occur."
- The ruling is one of the first court decisions to clarify the legal confusion between retailers and banks in data breaches. In the past, banks were often left with the financial burden of a hacking and were responsible for replacing stolen cards. The cost of replacing stolen cards from Target's breach alone is roughly $400 million.
- The Target ruling makes clear that banks have a right to go after merchants if they can provide evidence that the merchant may have been negligent in securing its systems.
- At the time of its breach last year, Target had installed a $1.6 million advanced breach detection technology from the company FireEye.
- But according to several people briefed on its internal investigation who spoke on the condition of anonymity, the technology DID SOUND ALARMS that Target ignored until hackers had already made off with credit and debit card information for 40 million

customers and personal information for 110 million customers.

Sony

- "GOP" - Guardians of Peace
- <quote>
    - We've got great damage by Sony Pictures.
    - The compensation for it, monetary compensation we want.
    - Pay the damage, or Sony Pictures will be bombarded as a whole.
    - You know us very well. We never wait long.
    - You'd better behave wisely.
    - From God'sApstls

November 25th:

- Via a Pastebin link.
- Torrent files hosted on four sites consisting of 26 parts, broken out into 25 1GB files, and one 894 MB rar file.
- The files were also uploaded to the file sharing giants MEGA and Rapidgator, but removed by site managers shortly after.
- Information on 4,000 past and present Sony employees.
- Brief eMail dialog between researchers at Risk Based Security and the GOP stated that over 12 TERABYTES of data had been obtained from Sony's servers and workstations.

November 26th:

- Torrent links were published to Torrent Trackers containing UNRELEASED MOVIES:
    - Annie (December 19)
    - Mr Turner (December 19)
    - To Write Love On Her Arms (March 2015)
    - According to several torrent tracking sites, these files have been downloaded over 100,000 times.

December 1st (Monday before last):

- NBC News reports that the FBI is investigating the breach.
- North Korea?
- Another 24.87 GB of data leaked:
    - 33,880 files and 4,864 folders.
    - 47,426 unique names and Social Security Numbers (SSN)
    - 15,232 SSN belonged to current or former Sony employees
    - 3,253 SSN appeared more than 100 times
    - 18 files contained between 10,860 and 22,533 SSN each.
- Example of employee data found:
    - One file (\HR\Benefits\Mayo Health\Mayo XEROX assessment feed) contains 402 full Social Security numbers, internal emails, plaintext passwords, and employee names.

    - An additional 3000 or more Social Security numbers, names, contact details, contact phone numbers, dates of birth, email addresses, employment benefits, workers compensation details, retirement and termination plans, employees previous work history, executive salaries, medical plans, dental plans, genders, employee IDs, sales reports, copies of passport information and receipts for travel, as well as ((oddly)) money order details to purchase movie tickets to resell back to the Sony staff. The leaked information also included documents, payment, and account information to order custom jewelry from Tiffany & CO via email.

December 3rd (last Wednesday):

- Sony had confirmed that the leak was authentic.
- GOP: "Today more interesting data will be presented for you."
- 1.18 GB containing two files named "Bonus.rar" and "List.rar"
- Containing the MOST SENSITIVE data released to this point:
    - Full Security Certificate information.
    - Inernal and External account credentials with plaintext passwords for Sony, YouTube page, UPS accounts, etc.

- BONUS.RAR summary:
    - 33.7MB compressed
    - Contains plaintext credentials (~ 500 total), server information, internal IP addresses and other data.
    - Security certificates for servers, users, and services, and a list of what each certificate is related to.
    - Credentials include YouTube login information for the SonyPictures, Spidermanmovie, EvilDeadMoive, GrownupsTheMovie, and Thisistheend movie channels, complete list of older social media accounts for campaigns on facebook and twitter.
    - 121 FTP plaintext credentials, including the main Sony Pictures FTP server.
    - Plain text Credentials for major news and media sites like NY times, LA Times, Daily Variety, hollywoodreporter.com, indiewire.com.
    - Plain text passwords in formats like “sony12345” for critical internal and forward facing services.
    - Username passwords combos in many "password" files all in clear text with username and passwords.
    - Accounting and payment information for AMEX for “The Interview” in plain text.
    - Accounting and payment and other related credentials for “Death at a Funeral”

- LIST.RAR file summary:
    - 1.8MB compressed
    - Three files containing internal and external PC data, Linux servers, and Windows servers logon credentials.

December 5th (Friday):

- The torrent is broken into 22 files spanning 52 parts which appear to be just over

100GB of compressed data.
- This leak has been titled "Financial data of Sony Pictures" so it likely contains financial details of Sony Pictures, the budgets of movies, or more.
- These 22 individual files make up three larger files containing a large set of newly released data, predominantly financial information:

- File One:
    - 30,916 individual Files, 2,970 Folders. 16.4 GB / 9.99 GB (Compressed)
    - Banking statements, bank account information including wire transfer swift codes etc.
    - Financial year reports
    - Financial year forecasts
    - Budget reports
    - Overhead reports
    - Receipt and transaction account statements of computer hardware, vehicles, car accessories going back to 1998.
    - Internal information for Sony Pictures Releasing International portal, screenshots, walkthroughs and other usage information.

- File Two:
    - 89,800 Files, 10,990 Folders. 88.6 GB / 48.9 GB (Compressed)
    - Accounting information using Trintech Inc. software.
    - Licensing contracts with
    - Access Digital (Exyflix)
    - Amazon Europe
    - Amazon Japan
    - Clickpay Multimedia
    - Comcast
    - Eagle Eye
    - Gaia
    - Google (YouTube)
    - Media Vault
    - M-GO
    - Microsoft
    - Playstation
    - Sena
    - Sony Electronics
    - Sony visual products in
    - video futur
    - Yota (aka more)
    - Vendors (Too many to list)
    - Sony India Financial reports.
    - 528 Payrolls for Imageworks Canada with staff full names, contact numbers and residential addresses.
    - British Columbia Personal Tax Credit Returns scans of employees with full personal information including social security number.
    - Photocopies and scans of driver licenses, passports and other tax related documents exposing personal credentials, home addresses, full names, date of

births, social security numbers and more.
    - Federal Tax Returns

- File Three:
    - 113,002 Files, 39,612 Folders. 57.1 GB. / 48.1GB (Compressed)
    - Incident reports with full names, incident locations, injurys and positions held with Sony.
    - UL training users, full names, addresses, email addresses and common set clear text passwords.
    - Copies of employeement contracts and agreements, passports, drivers license, ssn, signatures.

December 8th (Yesterday):

- Four archives making two large files, currently being seeded from servers owned by Sony Pictures as before.
- The torrent that includes all files is only 2.8GB this time and has also been uploaded to a few file sharing websites, although they are expected to be taken down quickly like previous GOP uploads.

- 05_01.rar
    - mosokos.ost (A Microsoft Outlook mail spool), 3.5GB in size
    - The file is corrupted, won't unpack.

- 05_A.rar
    - APascal1.ost (A Microsoft Outlook mail spool), 3.78GB in size
    - "APascal" is Amy Pascal, Co-Chairman, Sony Pictures Entertainment and Chairman, Sony Pictures Entertainment Motion Picture Group
    - Over 5,000 emails included
    - Most recent Inbox email is from November 23, 2014 (likely when the mail spool was taken)
    - Emails consist of sony employee relations, personal invoices, and personal emails
    - Includes talk and deals about upcoming movies
    - Contains current and closing business deals