Security Now! #488 - 12-30-14

The (In)Security of 2014

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!

- Who hacked Sony?
- Who blasted North Korea?
- Apple deploys their forced-update for the first time ever.
- The Lizard Squad takes down XBox Live and PSN.
- What the NSA apparently can and not decrypt.
- My thoughts on two movies
- A look back though a too-busy 2014...

SQRL:

- Last week's DigiCert/SQRL presentation
- SQRL: Now at the first-publication point…

Security News:

"No, North Korea Didn't Hack Sony"

- http://www.thedailybeast.com/articles/2014/12/24/no-north-korea-didn-t-hack-sony.html
- Marc Rogers:
  - Director of security operations for DEFCON, the world's largest hacker conference.
  - Principal security researcher for CloudFlare.
- Marc writes: The FBI was very clear in its press release about who it believed was responsible for the attack: "The FBI now has enough information to conclude that the North Korean government is responsible for these actions," they said in their December 19 statement, before adding, "the need to protect sensitive sources and methods precludes us from sharing all of this information".
- All but one of the IP addresses used are well-known open public proxies
  - 202.131.222.102—Thailand
  - 217.96.33.164—Poland
  - 88.53.215.64—Italy
  - 200.87.126.116—Bolivia
  - 58.185.154.99—Singapore
  - 212.31.102.100—Cyprus
  - 208.105.226.235—USA

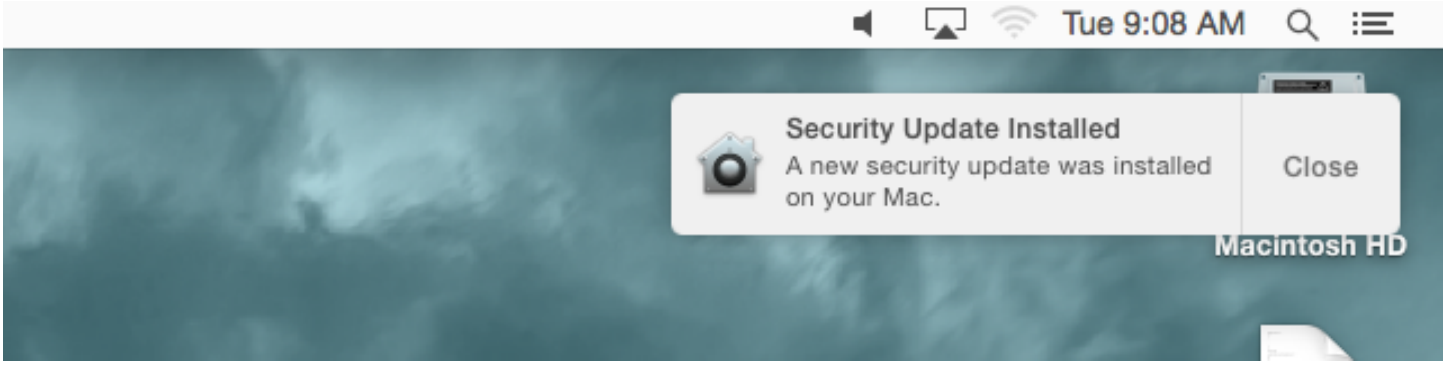
- Other Rationale:
    - First of all, there is the fact that the attackers only brought up the anti-North Korean bias of "The Interview" after the media did—the film was never mentioned by the hackers right at the start of their campaign. In fact, it was only after a few people started speculating in the media that this and the communication from North Korea "might be linked" that suddenly it did get linked.
    - The hackers dumped the data. Would a state with a keen understanding of the power of propaganda be so willing to just throw away such a trove of information? The mass dump suggests that whoever did this, their primary motivation was to embarrass Sony Pictures. They wanted to humiliate the company, pure and simple.
    - Blaming North Korea offers an easy way out for the many, many people who allowed this debacle to happen; from Sony Pictures management through to the security team that were defending Sony Picture's network.
    - You don't need to be a conspiracy theorist to see that blaming North Korea is quite convenient for the FBI and the current U.S. administration. It's the perfect excuse to push through whatever new, strong, cyber-laws they feel are appropriate, safe in the knowledge that an outraged public is fairly likely to support them.
    - Hard-coded paths and passwords in the malware make it clear that whoever wrote the code had extensive knowledge of Sony's internal architecture and access to key passwords. While it's (just) plausible that a North Korean elite cyber unit could have built up this knowledge over time and then used it to make the malware, Occam's razor suggests the simpler explanation of an upset insider. Combine that with the details of several layoffs that Sony was plannin,g and you don't have to stretch the imagination too far to consider that a disgruntled Sony employee might be at the heart of it all.

Monday, Dec 22nd... North Korean Internet (kinda) Collapses

- http://www.nytimes.com/2014/12/23/world/asia/attack-is-suspected-as-north-korean-internet-collapses.html
- On Friday, Obama gives his final press conference of the year, heads for Hawaii...
- Connection started becoming flaky late Friday, gradually worsened over the weekend, and was out by Monday.
- And Monday, NK Internet connectivity sputters and falters.
- A very weak Internet infrastructure.
- Anyone could have done it.
- 1024 IP addresses. David Sanger, New York Times:
    - Photo Caption: Kim Jong-un leads a country that has fewer Internet protocol addresses than many city blocks in New York.
- The State Department, when asked:
    - Marie Harf: "We aren't going to discuss, publicly, operational details about the possible response options. As we implement our responses, some will be seen, some may not be seen."

Apple deploys their OS 10 Auto-Patcher! (For the first time ever)

http://arstechnica.com/apple/2014/12/apple-automatically-patches-macs-to-fix-severe-ntp-security-flaw/



- NTP remote code execution buffer overrun.
- DHS / CERT:Products using NTP service prior to NTP-4.2.8 are affected.
    - https://ics-cert.us-cert.gov/advisories/ICSA-14-353-01A
- No specific vendor is specified because this is an open source protocol.
- <quote> A remote attacker can send a carefully crafted packet that can overflow a stack buffer and potentially allow malicious code to be executed with the privilege level of the ntpd process. All NTP4 releases before 4.2.8 are vulnerable.
- Privilege of the NTPD... often root.

It's been a WEIRD last few weeks!...

The Lizard Squad Attacks - Xbox Live & Playstation Network

- http://www.businessinsider.com/why-hacker-gang-lizard-squad-took-down-xbox-live-and-playstation-network-2014-12
- http://www.winbeta.org/news/exclusive-interview-cyber-terrorist-group-lizard-squad-why-they-brought-down-xbox-live-and-psn
- Learned from the Lizard Squad:
    - Taking down PlayStation Network and Xbox Live started "for the laughs," but eventually the collective found a cause to rally behind — forcing these companies to upgrade the security on their networks.
    - Lizard Squad chose Christmas Eve and Christmas Day because it believed "it would anger and reach the largest amount of people."
    - The gang considered taking down Nintendo's online service, but did not, with no particular reason given.
    - When asked if the group would consider addressing other targets, Lizard Squad said it "could take down NASDAQ if they wanted to damage the economy," but said that's not its goal.
    - The easier game network to take down was Microsoft's Xbox Live. Sony had apparently upgraded its security recently, which took "a bit of time to work around," but Microsoft had "almost nothing" in terms of security.
    - Lizard Squad has not said when the attacks would stop: It said they would continue until the companies "learned from their security issues."

- But then…
    - Kim Dotcom paid them (with vouchers for his Mega service) to lay off the game

networks.
    - The Lizard Squad tweeted their acknowledgement and thanks... and agreed.

Snowden docs reveal what causes NSA headaches

- http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html
- Der Spiegel: Prying Eyes: Inside the NSA's War on Internet Security
- Skype: Cracked and wide open:
    - Since February 2011, the service has been under order from the secret US Foreign Intelligence Surveillance Court (FISC), to not only supply information to the NSA but also to make itself accessible as a source of data for the agency.
- The NSA cryptologists divided their targets into five levels, corresponding to the degree of the difficulty of the attack and the outcome, ranging from "trivial" to "catastrophic."
    - Trivial / Minor / Moderate / Major / Catastrophic
- For example:
    - Trivial: Monitoring a document's path through the Internet.
    - Minor: Recording Facebook chat.
    - Moderate: Decrypting emails sent through Moscow-based Internet service provider "mail.ru".
- Things first become troublesome at the fourth level: “Major”
    - Decrypting messages sent through heavily encrypted email service providers like Zoho
    - Monitoring users of the Tor network
    - TrueCrypt
    - OTR - Off The Record protocol.
- Catastrophic
    - Simultaneous use of multiple systems... ZRTP (Zimmermans's phone encryption) over TOR.
- VPNs, SSL/TLS

Miscellany:

The Interview.

- Shockingly adolescent.

The Immitation Game

- Amazingly good!

The (In)Security of 2014

The Year in Review

- More NSA/US government spying revelations thanks to Edward Snowden
- Attacks on Consumers and Corporations and Governments

    - (by Governments and Malicious Hackers)
- Lots of vulnerabilities found in consumer and Internet equipment and protocols.

Names both well known and new:

- NSA & Snowden, P.F.Chang's, Target, Home Depot, Sony
- "Goto:Fail", TrueCrypt, Heartbleed, BadUSB, ShellShock, Poodle, Regin

A 2014 Internet Security Chronology

Entering into 2014:

- P.F.Chang's -- selected stores in the South East.
- Target: Consequences of the huge end-of-2013 Target breach:
    - 40 million credit cards stolen
    - 110 million customer's personal information compromised
- $400 million cost to the banks for CC replacement.
- Judge recently ruled that lawsuits against Target could proceed.

Serious "wide open" backdoor discovered in consumer routers by Cisco, Linksys, NetGear and others.

- Over the Christmas/New Year holiday.
- Simply connect to TCP port 32764.

Apple's "Goto:Fail"

- February 21st - iOS and Mac were not verifying certificates.
- Apple quietly issued a 'fix' and then went public.

TrueCrypt

- April 14th - Phase 1 of independent audit comes out 100% clean. (Yay!)

Heartbleed

- April 7th... discovery of a buffer overrun in OpenSSL affecting many many servers.
- Difficult to exploit requiring a lot of "chance". Initial skepticism.
- Shortly afterward remote credential capture was confirmed.

Intentional backdoor re-discovered in consumer routers (Cisco, Linksys, NetGear)

- April 21st - Now send a special Ethernet "knock" packet to unlock the backdoor.
- Hidden backdoors installed by vendors allowing remote access and full control.
- TCP port 32764
- The original backdoor allowed unrestricted/unauthenticated root access to a router by connecting to port 32764.
- The backdoor was traced back to components manufactured by Sercomm.

- Sercomm delivers parts for a number of name brand routers sold under the brands of Cisco, Linksys, Netgear, Diamond and possibly others.

TrueCrypt

- May 29th - TrueCrypt developers decide to throw in the towel. (Boo!)
- Many people put off by the somewhat bizarre way the TC devss bailed.

"BadUSB"

- August BlackHat presentation frightened everyone that USB firmware was re-writable.
- Many USB thumbdrives could be made malicious.

Google declares war on SHA-1 certificates

- September 5th
- Plans to start punishing websites (two years early) whose certs are signed with SHA-1.

Home Depot

- September 18th
- Home Depot: 56 million credit cards compromised

Shellshock (aka "bashdoor")

- Sept 24th - the ubiquitious BASH Unix/Linux shell executes commands in environment variables!
- Many Internet-exposed services silently use the shell in the bacground.
- A worm and botnets were quickly created (and are busy now!)

Poodle - (Padding Oracle On Download Legacy Encryption)

- October 17th
- We've moved on to TLS (v1.0, v1.1, v1.2) but had left SSL v3.0 for backwards compatibility.
- That turned out not to be okay. Falling back to SSLv3 could theoretically allow for the slow decryption of (session) cookies.

"Regin"

- November 23rd - New super-powerful state-sponsored espionage software.
- Probably Russian in origin. Kaspersky and Symantec had been tracking "something" for years.

Poodle Bites (again)

- December 8th - 10% of websites still vulnerable due to Internet-facing appliances still running SSLv3.0.
- Appliance devices didn't get updated… but they were still running vulnerable stacks.

Sony's Mega-Hack

- A wake up call for corporate security???

But... some GOOD NEWS for the consumer:

In the wake of the Snowden/NSA revelations…

- Apple and Google have both decided to hugely improve their user's and device's security.
- Many truly secure communications solutions have been offered
- Many more are on the horizon.