

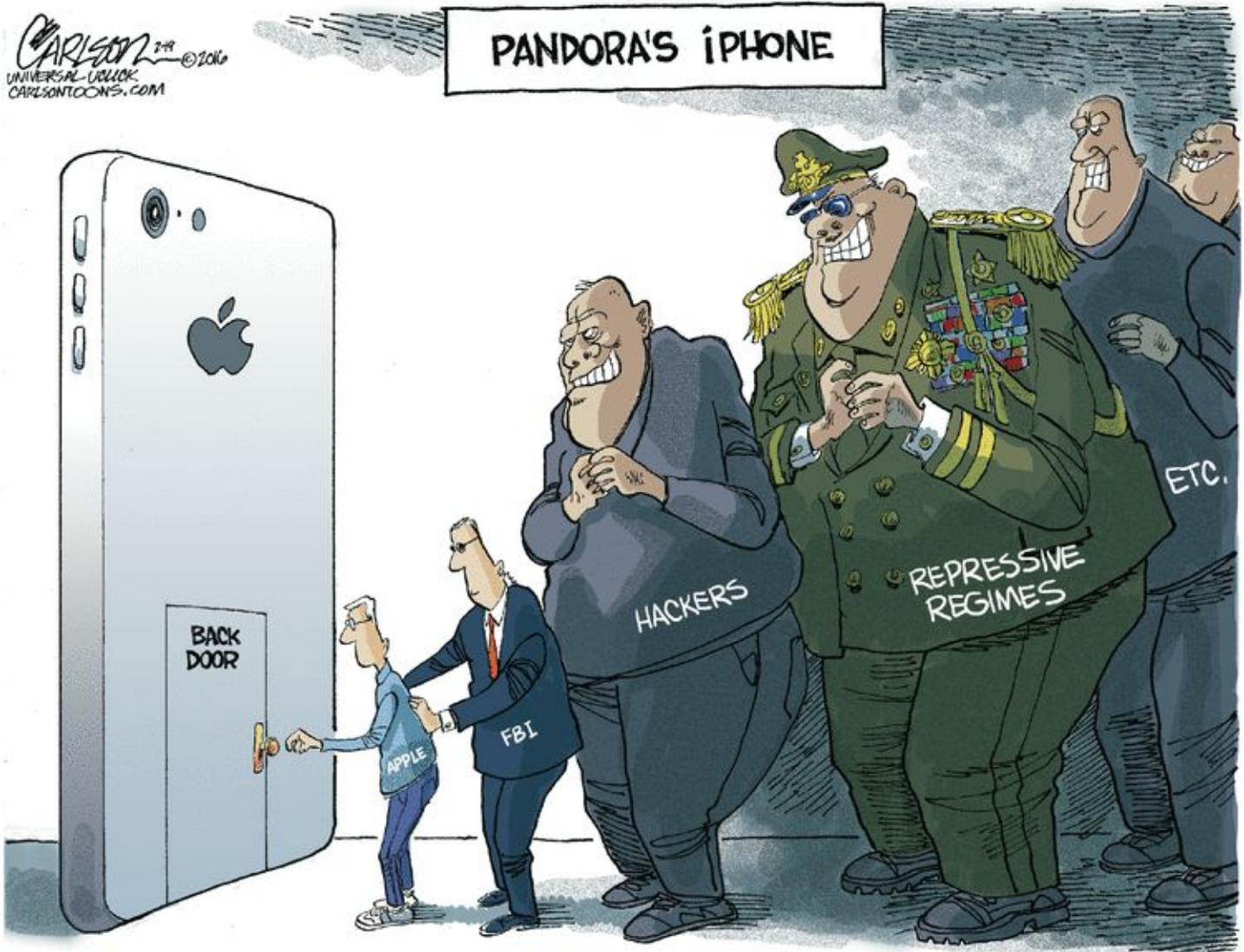
# Security Now! #548 - 02-23-16

## DDoS Attack Mitigation

### This week on Security Now!

- Apple vs The FBI
- Linux Mint
- More Comodo bad news
- Hollywood Presbyterian Medical Center pays Crypto ransom
- Glibc flaw follow-up
- Error 53 follow-up

CARLSON 2/19 ©2016  
UNIVERSAL-UNLUCK  
CARLSONTOONS.COM



# Security News

## Apple vs The Courts

Requesting three changes:

- Remove the 10 mistake lockout
- Remove additional software-induced per-attempt delays.
- Allow for high-speed automated guessing.
  - Hardware imposes an 80 ms per-attempt delay.

Remember:

- iOS installs ARE per-device:
  - Upon connection, device requests an update.
  - Device provides its unique ID + nonce.
  - Apple \*must\* sign this unique per device and per interchange request.
  - Signature of this unique per device and per request packet MUST verify with burned-in public key.
- LOCKED devices WILL update.

NPR: Senator Angus King says that congress should decide encryption (4min:35sec)

- <http://bit.ly/sn-548-2>
- <http://www.npr.org/2016/02/19/467318832/congress-should-decide-encryption-issue-sen-angus-king-says>
- Steve Inskeep interviews senator Angus King

Manhattan district attorney Cyrus Vance Jr.

- <http://bit.ly/sn-548-1>
- <http://www.npr.org/2016/02/21/467547180/it-s-not-just-the-iphone-law-enforcement-wants-to-unlock>
- Cyrus tells NPR's Rachel Martin that his cyberlab has asked Apple to break into 175 phones.

Matthew Green: Why can't Apple decrypt your iPhone?

- <http://blog.cryptographyengineering.com/2014/10/why-cant-apple-decrypt-your-iphone.html>
- I wrote this blog post on Apple iPhone encryption a while back. To my knowledge, it's still an accurate description.
- What these stories show is that Apple's encryption protections mostly work, and that the DoJ is willing to push as hard as it can.

- Apple's main protection is an 80ms per password-attempt delay that is enforced by tamper resistant hardware. And it works.
- Stuff like the ten-attempt limit and throttling delays are probably all enforced by software and Apple can almost certainly turn them off.

#### Tim Cook vs the FBI

- [http://www.theregister.co.uk/2016/02/17/why\\_tim\\_cook\\_is\\_wrong\\_a\\_privacy\\_advocates\\_view/](http://www.theregister.co.uk/2016/02/17/why_tim_cook_is_wrong_a_privacy_advocates_view/)

#### Google's CEO just sided with Apple in the encryption debate

- <http://www.theverge.com/2016/2/17/11040266/google-ceo-sundar-pichai-sides-with-apple-encryption>

#### Timeline:

- <http://www.theverge.com/2016/2/17/11032612/apple-fbi-open-letter-future-of-iphone-security/in/10800347>
- <http://www.theverge.com/2016/2/17/11031910/donald-trump-apple-encryption-backdoor-statement/in/10800347>
- <http://www.theverge.com/2016/2/17/11035296/apple-iphone-encryption-fight-security-fbi/in/10800347>
- <http://www.theverge.com/2016/2/17/11036642/whatsapp-apple-defense-fbi-encryption-battle/in/10800347>
- <http://www.theverge.com/2016/2/17/11037838/us-congress-awa-encryption-debate-apple-fbi-battle/in/10800347>
- <http://www.theverge.com/2016/2/17/11040266/google-ceo-sundar-pichai-sides-with-apple-encryption/in/10800347>

#### Facebook, Twitter side with Apple in iPhone fight

- <http://www.usatoday.com/story/tech/news/2016/02/18/facebook-support-apple-iphone-san-bernardino-fbi/80578754/>

#### Apple Gets An Extension In iPhone Unlock Case, Response Now Due February 26th

- <http://techcrunch.com/2016/02/18/apple-gets-an-extension-in-iphone-unlock-case-response-now-due-february-26th/>

#### The iPhone Technology

- <http://arstechnica.com/apple/2016/02/encryption-isnt-at-stake-the-fbi-knows-apple-already-has-the-desired-key/>

## Upgrade Your iPhone Passcode to Defeat the FBI's Backdoor Strategy

- <https://theintercept.com/2016/02/18/passcodes-that-can-defeat-fbi-ios-backdoor/>

## **Warning! — Linux Mint Website Hacked and ISOs replaced with Backdoored Operating System**

- <http://thehackernews.com/2016/02/linux-mint-hack.html>
- <http://www.zdnet.com/article/hacker-hundreds-were-tricked-into-installing-linux-mint-backdoor/>
- Sat, Feb. 20th: Malicious ISO images for the Linux Mint 17.3 Cinnamon Edition
- Zack Whittaker for ZDNet's Zero Day...
- The hacker said their prime motivation for the backdoor was to build a botnet.
- Linux Mint distro, compromised for a day, last Saturday.
  - (About 6 million users of the Mint distro.)
- The hacker responsible, who goes by the name "Peace," told Zack, in an encrypted chat on Sunday, that a "few hundred" Linux Mint installs were under their control -- a significant portion of the thousand-plus downloads from the day.
- The Linux Mint forum was also breached:
  - its entire content obtained,
  - and its PHPass hash is insufficiently strong to prevent hash cracking.
- Zack explains how the hack was performed, then notes:  
"The hacker then used their access to the site to change the legitimate checksum -- used to verify the integrity of a file -- on the download page with the checksum of the backdoored version.:"
- The hacker said there was no specific goal to their attack, but said that their prime motivation for the backdoor was to build a botnet.
- The hacker used malware dubbed Tsunami, an easy-to-implement backdoor, which when activated quietly connects to an IRC server where it waits for commands.
- Tsunami is a simple manually configurable bot which talks to an IRC server and joins a predefined channel, with a password if set by the creator. But it isn't just used to launch web-based attacks, it can also allow its creator to execute commands and download files to the infected system for later execution.
- It can also uninstall itself to remove evidence of its previous presence.

## **Comodo Internet Security installs and starts a VNC server by default**

- <https://code.google.com/p/google-security-research/issues/detail?id=703>
- Tavis Ormandy:  
When you install Comodo Internet Security, in the default configuration an application called "GeekBuddy" is also installed and added to HKLM\System\CurrentControlSet\Services.
- GeekBuddy is a tech support application, that uses a number of questionable and shady tactics to encourage users to pay for online tech support.  
<https://www.comodo.com/home/support-maintenance/geekbuddy.php>  
(Yeah... for \$200/year!)
- As has been noted by numerous people over the last few years, GeekBuddy also installs a VNC server and enables it by default.  
(VNC is a popular free remote desktop facility.)

## **Hollywood Presbyterian Medical Center (HPMC) pays \$17k for ransomware crypto key**

- <http://arstechnica.com/security/2016/02/hospital-pays-17k-for-ransomware-crypto-key/>
- Hollywood Presbyterian says systems were restored after 10-day lockout.
- After 10 days without access to patient records, hospital pays 40 bitcoins - \$17,000 USD.
- In a published statement, Allen Stefanek, President & CEO wrote:  
"The first signs of trouble at HPMC came on February 5, when hospital employees reported being unable to get onto the hospital's network. Our IT department began an immediate investigation and determined we had been subject to a malware attack. The malware locked access to certain computer systems and prevented us from sharing communications electronically.

Law enforcement was immediately notified. Computer experts immediately began assisting us in determining the outside source of the issue and bringing our systems back online.

The hospital staff was forced to move back to paper, and transmit information to doctors and others by fax machine while the IT team and outside consultants struggled to restore the network. Eventually, hospital executives decided that the quickest and most efficient way to restore our systems and administrative functions was to pay the ransom and obtain the decryption key. In the best interest of restoring normal operations, we did this."

## **Glibc Flaw Follow-up:**

- Dan Kaminsky: A Skeleton Key of Unknown Strength
  - Dan discovered the problem with DNS server spoofability due to poor entropy.
  - I created GRC's DNS spoofability test to allow anyone to check the entropy of the DNS servers being used to resolve their queries.

- <http://dankaminsky.com/2016/02/20/skeleton/>

The glibc DNS bug (CVE-2015-7547) is unusually bad. Even Shellshock and Heartbleed tended to affect things we knew were on the network and knew we had to defend. This affects a universally used library (glibc) at a universally used protocol (DNS). Generic tools that we didn't even know had network surface (sudo) are thus exposed, as is software written in programming languages designed explicitly to be safe. Who can exploit this vulnerability? We know unambiguously that an attacker directly on our networks can take over many systems running Linux. What we are unsure of is whether an attacker anywhere on the Internet is similarly empowered, given only the trivial capacity to cause our systems to look up addresses inside their malicious domains.

We've investigated the DNS lookup path, which requires the glibc exploit to survive traversing one of the millions of DNS caches dotted across the Internet. We've found that it is neither trivial to squeeze the glibc flaw through common name servers, nor is it trivial to prove such a feat is impossible. The vast majority of potentially affected systems require this attack path to function, and we just don't know yet if it can. Our belief is that we're likely to end up with attacks that work sometimes, and we're probably going to end up hardening DNS caches against them with intent rather than accident. We're likely not going to apply network level DNS length limits because that breaks things in catastrophic and hard to predict ways.

## **Error 53 Follow-up:**

Oops!

<https://support.apple.com/en-us/HT205628>

<quote> After you try to update or restore your iOS device in iTunes on your Mac or PC, you might see error 53 in iTunes and "Connect to iTunes" on your device. Error 53 appears when a device fails a security test. This test was designed to check whether Touch ID works properly before the device leaves the factory, and wasn't intended to affect customers.

For anyone who experienced error 53, Apple has released an update to iOS 9.2.1 to allow you to successfully restore your device using iTunes on your Mac or PC. Use the steps in this article to restore and recover your device. If you believe that you paid for an out-of-warranty device replacement based on an error 53 issue, contact Apple Support to ask about reimbursement.

Security Now! Follower... Dale Perkel (@PerkX)

#error53 followup

Steve, thanks for reading out my DM verbatim, I was thrilled to hear my name and what you and Leo had to say about Error 53 and my comments. I'm ecstatic that Apple has heard our collective calls and rectified the problem, it's exactly what we all wanted. They have done this without diminishing security and without compromising users! Just a note on the so called "3rd party repairers". It's true that we are not able to buy parts from Apple, unfortunately this is the way that they control the supply chain however parts tend to find ways out of factories in China which we are able to purchase. Most parts are of an equal quality to that of the original apple part, but inferior parts do exist and not all 3rd parties will install the highest quality parts either by choice or because of availability / supply. If repairing with Apple was possible everywhere, that is always the first choice but unfortunately in many parts of the world, only 3rd parties are available to repair Apple products. I hope your problems with grc.com are now behind you, thanks again and best regards to yourself and Leo! Cheers, Dale

## Miscellany

### **DigiCert, Inc. (@digicert)**

- DigiCert is looking for a new Customer Relations Intern - check out details and where to turn in résumé here: [buff.ly/1Q90sU9](http://buff.ly/1Q90sU9)
- DigiCert Jobs - Customer Relations Intern
- <https://www.digicert.com/news/jobs/customer-relations-intern.htm>
- <http://bit.ly/digicertjob>

### **David Needle died.**

- <http://www.develop-online.net/news/co-creator-of-amiga-1000-atari-lynx-and-3do-dave-needle-passes-away/0216908>

### **OMG! TiVo just added instant commercial skip!**

- It works amazingly well!

## SpinRite

### Fred Pollock

Location: Goodrich, Mi. (No I'm not on Flint water)

Subject: Zeo still available on E-bay 02/10/2016 as of 9:00pm eastern time

Date: 10 Feb 2016 18:34:37

:

I just watched your latest PodCast on TWIT. I thought I had missed my chance to get a Zeo. Not true, \$40.00 and it is on it's way.

Great PodCast Steve and Leo. I have been a listener from almost the first one. I use a Roko now. The app works great. Thanks Again.

I have owned SpinRite for years and can't count the number of creaky hard drives it's brought back to life (just like the Terminator Movie) They just get up and go again. Sometimes it gets a little scary like a zombie you can't kill. (Good Zombie Good Zombie) LOL

---

## DDoS Attack Mitigation

**First off: I have done NOTHING to get us back on the Internet.**

### The past week with attacks and Level3

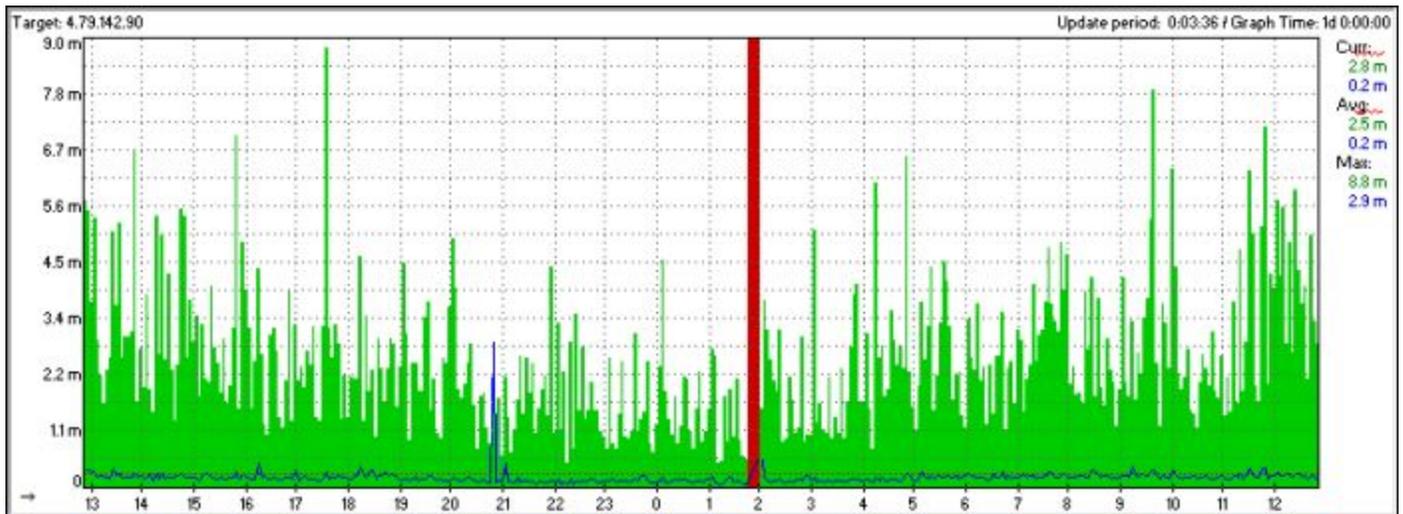
- First hit Saturday before last, 3 times.
- 90 minutes, 60 minutes... three hours off, then again.
- Level3 shut us down because our traffic was hurting the neighborhood.
- We were sharing a Cisco router which had a 10 Gbps connection.

### Filtering vs Flooding

- Initially just DNS aimed at port 53
- Later, UDP fragments, TCP ACKs and the kitchen sink.
- Routing and Null-Routing
  - Null routed grc.com and www.grc.com came back up.
  - Attacker was watching and moved to www.grc.com.
  - Added a null route for www.grc.com and newsgroups came back.
  - Attacker was watching and attacked something else.
  - I gave up and had Level3 shut us down.
  - While down... we're completely blind.

## Opened a dialog with Level3's DDoS / Security people.

- Thursday evening... down for the count.
- Came up Friday and was fine all day Friday and Saturday.
- Saturday night / Sunday morning, just past midnight.
- Monday I confirmed that our Level3 bandwidth had been "groomed"
- This (Tuesday) morning from 1:45am to 2am.



## The response from every quarter

- DDoS solution providers:
  - Cloudflare, Incapsula, Russia's largest DDoS mitigator
  - SN podcast listeners
  - Level3's internal staff of heroes.
    - (Bryce, Brandon, Sharon, Lee, Tim, Robert, and others.)

## Who's behind it?

- 64.40.0.0 /20 - PalTalk's network
- Ultimately, I don't care.
- 2001 / Wicked / Michael / FBI

## Three aspects of Mitigation

- Web services
  - Must be hidden behind big-pipe reverse proxies
  - Those proxies have GRC's DNS... and terminate TLS connections!
  - Thus... they are OITM (organization in the middle) **with GRC's certs!!**
  - "But that's what everyone does!"
- TCP servers: eMail + NNTP newsgroups
- GRC's unique custom services