From: Richard Kahn <[redacted]>
Sent: Tuesday, March 29, 2016 9:56 PM
To: jeffrey E.

james commentary on apple / fbi situation

Richard Kahn
HBRK Associates Inc.
575 Lexington =venue 4th Floor
New York, NY 10022
tel [redacted]
fax [redacted]
cell [redacted]

Begin forwarded message:

From: =/b>james | personal genius <[redacted]>

Subject: =/b>Re:

Date: =/b>March 29, 2016 at 5:32:36 PM =DT

To: =/b>Richard Kahn <[redacted]>

One more thing of note, had the FBI / DOJ =revailed in court, they'd have wide reaching new powers to compel =hird-parties to act on their behalf, even at the expense of the =hird-parties' self interest.

They could, for example, have a court =ompel me to install tracking software on Jeffrey's systems and forbid =e from disclosing it. Not that they could actually get me to do =omething like that, but it's within their proposed legal =ustification.

Also relevant is this: https://www.washingtonpost.com/news/the-watch/wp/2016/03/10/sur=rise-nsa-data-will-soon-routinely-be-used-for-domestic-policing-that-has-=othing-to-do-with-terrorism/

The surveillance state is not just for =errorism anymore.

Thank you,

On Mar 29, 2016, at 5:19 PM, Richard Kahn =[redacted]>
> wrote:

interesting,,
thanks

Richard Kahn
HBRK Associates Inc.
575 Lexington =venue 4th Floor
New York, NY 10022
tel =[redacted]
fax[redacted]
cell [redacted]

On Mar 29, 2016, at 4:22 PM, james ce | personal genius =[redacted]
<mailto[redacted]> > wrote:

There are two =ikely methods* that could have been used to access the data on that =hone:

1. An =npublished "zero-day" bug that allows hackers to bypass =he lock screen and access encrypted data on the phone.

2. A =ardware solution where the memory chip (the flash storage on the phone) =as un-soldered from the logic board, and plugged into a machine that =an read / write the data from the chip (this is not new, this method =as actually used in the 1985 movie "Real Genius"), =hich then duplicated the data on the chip and simulated the =hone's hardware.

With that setup you can brute-force try =ll four-digit passcode options. When the device slows down/erases the =ata from too many failed attempts, you just copy it over and pickup =here you left off. Depending on how much data / size of the flash =emory chip, you can restore the original data in 5-20 =inutes.

The =econd method is MUCH more likely to have been used. It will work on any =Phone that does NOT have a fingerprint reader. Touch ID relies on a =secure enclave" chip that manages the login attempts and would =e effectively impossible to impersonate — so this method is =omething that Apple is aware of and has considered.

*there's a third method called "de-capping=E2�� which involves using microlasers to sear off the top of the =PU to read the device's unique identifier, which is the much =ore complex part of the two-part encryption key that the iPhone =ses.

Basically, =pple uses this hardware device ID combined with the passcode as the key =o encrypt the data. With the device ID, they can try to decrypt the raw =ata from the flash module within 10,000 tries.

The problem is that de-capping is very risky =amp; fragile. If you cut a micron too deep you destroy the identifier =ou're looking for and there's no possibility of =ecovering the data in anyway after. This makes this method practically =seless for any legal inspection.

We'll never know which, if either method was used �=94 or even if any relevant data was recovered. Since the suspects are =ead, any evidence recovered from the phone and the methodology used to =ccess it will never be entered into any court case.

If the first method was =sed and such a zero-day does exist — then yes, a "hacker =rmy" could have been theoretically unleashed on Apple. In that =ituation, it's very likely we'll see it used in a =uture public jailbreak method to break into the OS — hackers =re notoriously bad at keeping secrets, being that exposing secrets is =he primary motivation for most hackers — at which point =pple will find out about it and fix it.

——

It's at least =qually as likely that the whole "we broke in without Apple'= help" story is complete fiction that the FBI / DOJ used it as =n excuse to bail from a case that was going to make them look like =echnical incompetents, and would be lost, setting the precedent they =ant in the wrong direction.

The last brief Apple filed exposed some =ajor technical inaccuracies in the DOJ briefs, and any hearing would =ave included Apple Engineers schooling the courts on the basics of how =ncryption works and embarrassed the FBI's technical =esources.

Also,=remember that this iPhone belonged to the terrorist's employer. =oth he & his wife had personal cell phones and computers which they =estroyed the day of the attack. The iCloud backup of this phone from a =ouple weeks previous to the attack revealed NO personal email, text =essages or any other internet accounts on the device. It's very =nlikely that iPhone was ever used for anything outside of work or =ontains anything of value to investigators.

This case was never =bout anything on that phone, rather it was a hot-button political case =o expand the government's investigatory powers.

(Also, contrary to that article's subheading, =he FBI never asked for Apple to unlock the phone before pursuing legal =rders... that sounds nitpicky, but were they actually concerned =ith the contents of the device, you'd expect the FBI to ask =icely before trying to force-conscript private corporate resources into =ewriting the device's operating system.)

I =et this will come up again as soon as the FBI's newest toys =top working, but next time it will be an Android device in hopes that =oogle won't raise as much of a fuss as Apple.

On Mar 29, 2016, at 3:27 PM, Richard Kahn <[redacted]> wrote:

http://www.thedailybeast.com/articles/2016/03/29/did-the-fbi-ju=t-unleash-a-hacker-army-on-apple.html

thoughts?

Richard Kahn
HBRK Associates Inc.
575 Lexington =venue 4th Floor
New York, NY 10022
tel =[redacted]
fax[redacted]
cell [redacted]

=