

Ways to Hack the Badge

...and a few other goodies

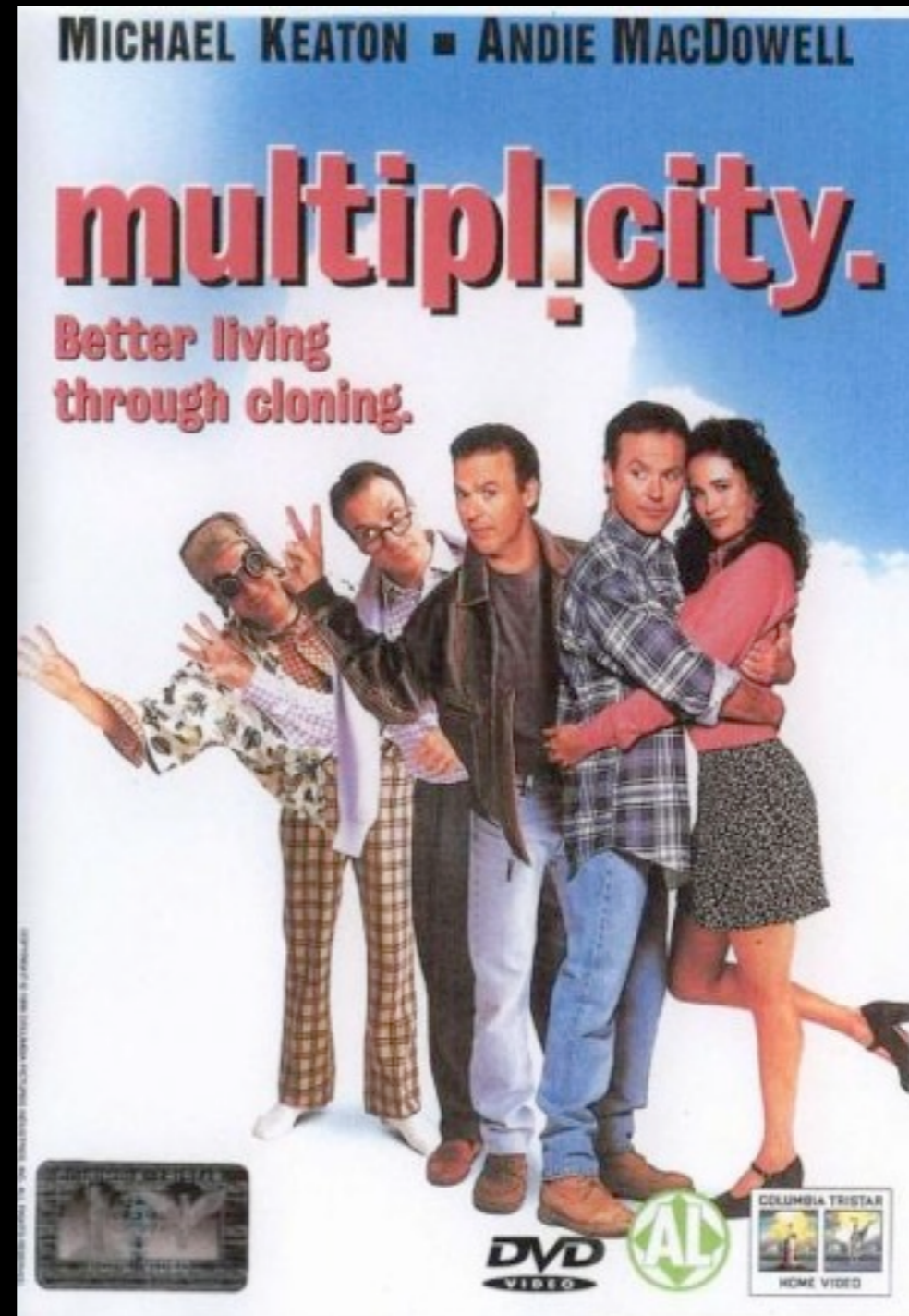
Surprise!

- Some teams interested in the RFID badge
- Fewer still with the reader itself
- One asked how they could SECURE the system...
 - Fail open
 - Cloning prevention
 - Auditing access
 - Re-writing tags non sequentially
 - Removing tags from the system*
 - Removing administrative rights
- Often the case in industry, they forget about the importance of physical security
 - While I was telling you about the badge, Red Team had cloned their first badge....

Surprise, did I scare you?



Clone a badge



Cloning

- Read and reprogram
- Obtain badge IDs from an insider
- Social engineering

```
the-hammer:~/Desktop/RFIDIOt-1.0a# ls -la | grep hid
-r-x 1 lpesce lpesce 2176 2009-11-30 06:46 hidprox.py
the-hammer:~/Desktop/RFIDIOt-1.0a# ./hidprox.py
.py hitag2brute.py hitag2reset.py
the-hammer:~/Desktop/RFIDIOt-1.0a# ./hidprox.py
v0.1c (using RFIDIOt v1.0a)
r: ACG LFX 1.0 (serial no: 14070051)

type not supported!
the-hammer:~/Desktop/RFIDIOt-1.0a# ./unique.py CLONE
v0.1j (using RFIDIOt v1.0a)
er: ACG LFX 1.0 (serial no: 14070051)

g for Unique tag...
```

root@the-hammer: ~/... | lpesce@the-hammer: ~

Cloning

- I told you I had a bunch of bits, an intergalactic rocket ship and various lengths of wire...



Hardware hack



PHOTOGRAPHERS
DIRECT.COM

<http://pauldotcom.com>

March 2009

Serial Output

- Exposed serial output from RFID reader
- Obtain RFID tag #'s from serial LCD



Replace Code



failblog.org

Upload

- Take apart to determine pins in use
- Rewrite new implementation
 - Need to obtain all tag #s, or forced reload
 - Go green regardless of tag!
- Upload some code via exposed USB port



Social Engineering

HACKERS CAN TURN YOUR HOME COMPUTER INTO A BOMB

By RANDY JEFFRIES / Weekly World News

WASHINGTON — Right now, computer hackers have the ability to turn your home computer into a bomb and blow you to Kingdom Come — and they can do it anonymously from thousands of miles away!

Experts say the recent "break-ins" that paralyzed the Amazon.com, Buy.com and eBay websites are tame compared to what will happen in the near future.

Computer expert Arnold Yehenson, president of the Washington-based consumer group National CyberCrime Prevention Foundation (NCCPF), says that as far as computer crime is concerned, we've only seen the tip of the iceberg.

"The criminals who knocked out those three major online businesses are the least of our worries," Yehenson told Weekly World News.

"There are brilliant but unscrupulous hackers out there who have developed technologies that the average person can't even dream of. Even people who are familiar with



Sickos can wreak death and destruction from thousands of miles away!

Arnold Yehenson.

low computers work have trouble getting their minds around the terrible things that can be done.

"It is already possible for an assassin to send someone an e-mail with an innocent-looking attachment connected to it. When the receiver downloads the attachment, the electrical current and molecular structure of the central processing unit is altered, causing it to blast apart like a large hand grenade.

... & blow your family to smithereens!



KABOOM! It might not look like it, but an innocent home computer like this one can be turned into a deadly weapon.

"As shocking as this is, it shouldn't surprise anyone. It's just the next step in an ever-escalating progression of horrors conceived and instituted by hackers."

Yehenson points out that these dangerous sociopaths have already:

- Vandalized FBI and U. S. Army websites.
- Broken into Chinese military networks.
- Come within two digits of cracking an 82-digit Russian security code that would have sent deadly missiles hurtling toward five of America's major cities.

"As dangerous as this technology is right now, it's going to get much

scarier," Yehenson said.

"Soon it will be sold to terrorists, cults and fanatical religion-fringe groups.

"Instead of blowing up a single plane, these groups will be able to patch into the central computer of a large airline and blow up hundreds of planes at once.

"And worse, this e-mail bomb program will eventually find its way into the hands of anyone who wants it.

"That means anyone who has a quarrel with you, holds a grudge against you or just plain doesn't like your looks, can kill you and never be found out."

Unlikely

- Possible, but I'd have to play real dumb
- This would make almost all of the attacks possible...
- So, try something else



Social Media



Welcome to the Social

- This one is a killer!
- Before we even showed up you could have found:
 - Pictures of the badge
 - Two suspected RFID tag types
 - Reader and writer hardware and software
 - Badge reader components
 - Almost working code
- All via Twitter, Facebook and Delicious and YouTube
 - Did not leak badge Unique IDs, but
 - An insider could have been leveraged (determined via twitter)
 - podcast/video often discusses RFID
 - Or, some recon on the PaulDotCom
- It is important to do some due diligence on your vendor because attackers will too.

Proof

Ahh, the smell of burning acrylic... <http://tweetphoto.com/13369538>

8:52 PM Mar 5th via TweetDeck

Proof

Ahh, the smell of burning acrylic... <http://tweetphoto.com/13369538>

8:52 PM Mar 5th via TweetDeck

Anyone know where I can order, in stock 100 RFID tags. Either HITAG 2 or S or Q5. Need on short notice.

2:00 PM Feb 18th via TweetDeck

Proof

Ahh, the smell of burning acrylic... <http://tweetphoto.com/13369538>

8:52 PM Mar 5th via TweetDeck

Anyone know where I can order, in stock 100 RFID tags. Either HITAG 2 or S or Q5. Need on short notice.

2:00 PM Feb 18th via TweetDeck

Ok, I'm impressed. The RFID tags that I ordered from Turkey this morning have already shipped.

12:10 PM Feb 19th via TweetDeck

Proof

Ahh, the smell of burning acrylic... <http://tweetphoto.com/13369538>

8:52 PM Mar 5th via TweetDeck

Anyone know where I can order, in stock 100 RFID tags. Either HITAG 2 or S or Q5. Need on short notice.

2:00 PM Feb 18th via TweetDeck

Ok, I'm impressed. The RFID tags that I ordered from Turkey this morning have already shipped.

12:10 PM Feb 19th via TweetDeck

23 FEB 10 [Arduino Forum - RFid checking tag number against tag number list](#) SAVE

Proof

haxorthematrix rfid x Type another tag

23 FEB 10 [Arduino Forum - Rfid checking tag number against tag number list](#) SAVE

18 FEB 10 [125 KHz RFID Card - Q5 ISO \(Re-Writeable\)](#) SAVE

[RFID USA - One Source for RFID - Radio Frequency Identification - RF](#)

<http://www.remoteidentity.com/search?query=q5&commit=Search> SAVE

16 JAN 10 [125 kHz Low Frequency \(LF\) Glass RFID Tag Hitag-S - Passive \[11100](#)
[Test](#) SAVE
Dial Ext. 601 for Sales

24 DEC 09 [RFID-Zapper\(EN\) - 22C3](#) SAVE

23 DEC 09 [codeninja.de - A scifi-gun that can fry electronics](#) SAVE

21 OCT 09 [Parallax RFID Reader Arduino](#) SAVE

05 OCT 09 [RFID Card Reader USB](#) SAVE

[USB-RS232-PCB Converter](#) SAVE



Proof

haxorthematrix rfid x Type another tag

23 FEB 10 [Arduino Forum - Rfid checking tag number against tag number list](#) SAVE

18 FEB 10 [125 KHz RFID Card - Q5 ISO \(Re-Writeable\)](#) SAVE

[RFID USA - One Source for RFID - Radio Frequency Identification - RF](#)

<http://www.remoteidentity.com/search?query=q5&comm>

16 JAN 10 [125 kHz Low Frequency \(LF\) Glass RFID Tag Hitag-S - Test](#) SAVE
Dial Ext. 601 for Sales

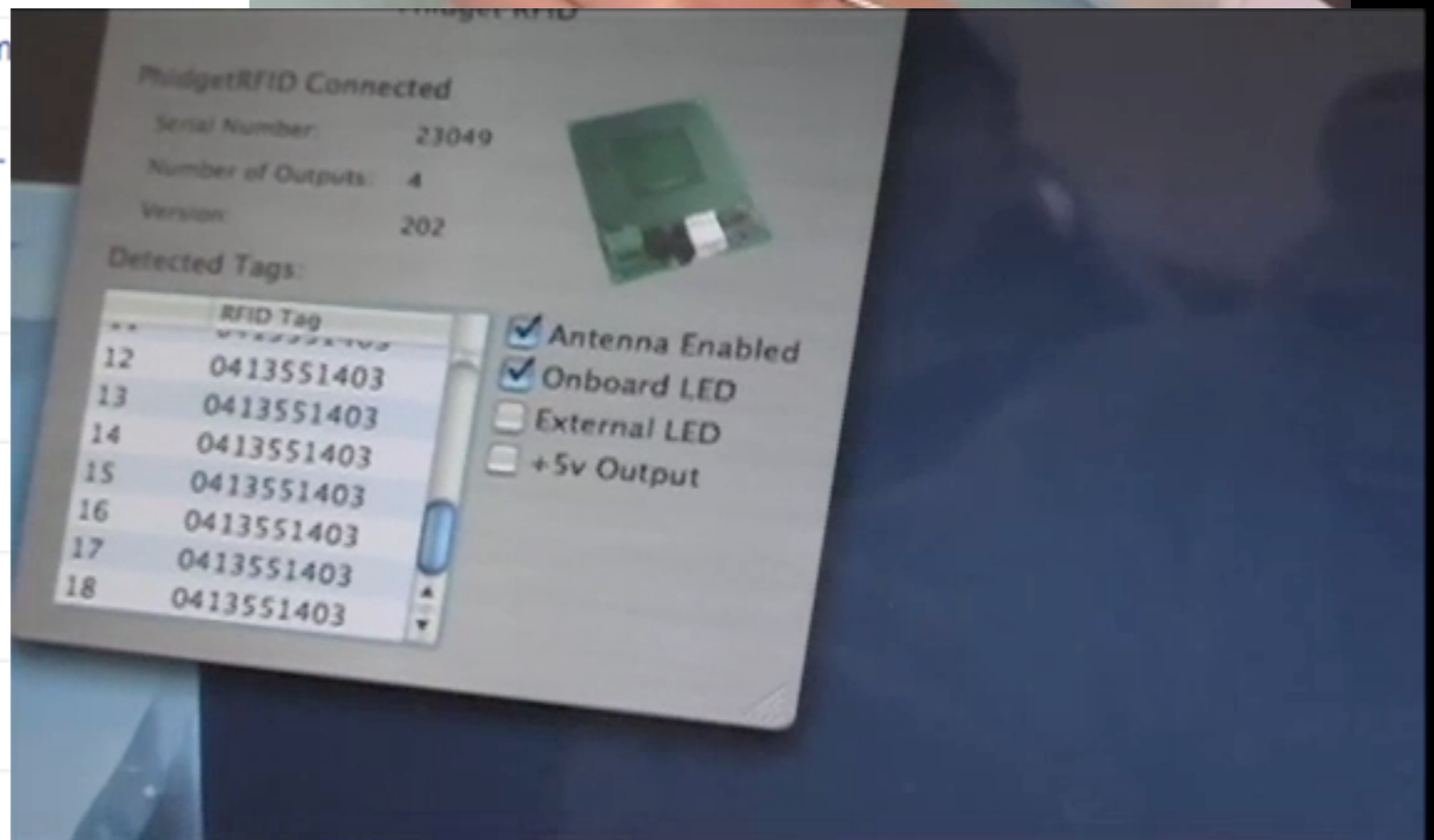
24 DEC 09 [RFID-Zapper\(EN\) - 22C3](#) SAVE

23 DEC 09 [codeninja.de - A scifi-gun that can fry electronics](#) SAVE

21 OCT 09 [Parallax RFID Reader Arduino](#) SAVE

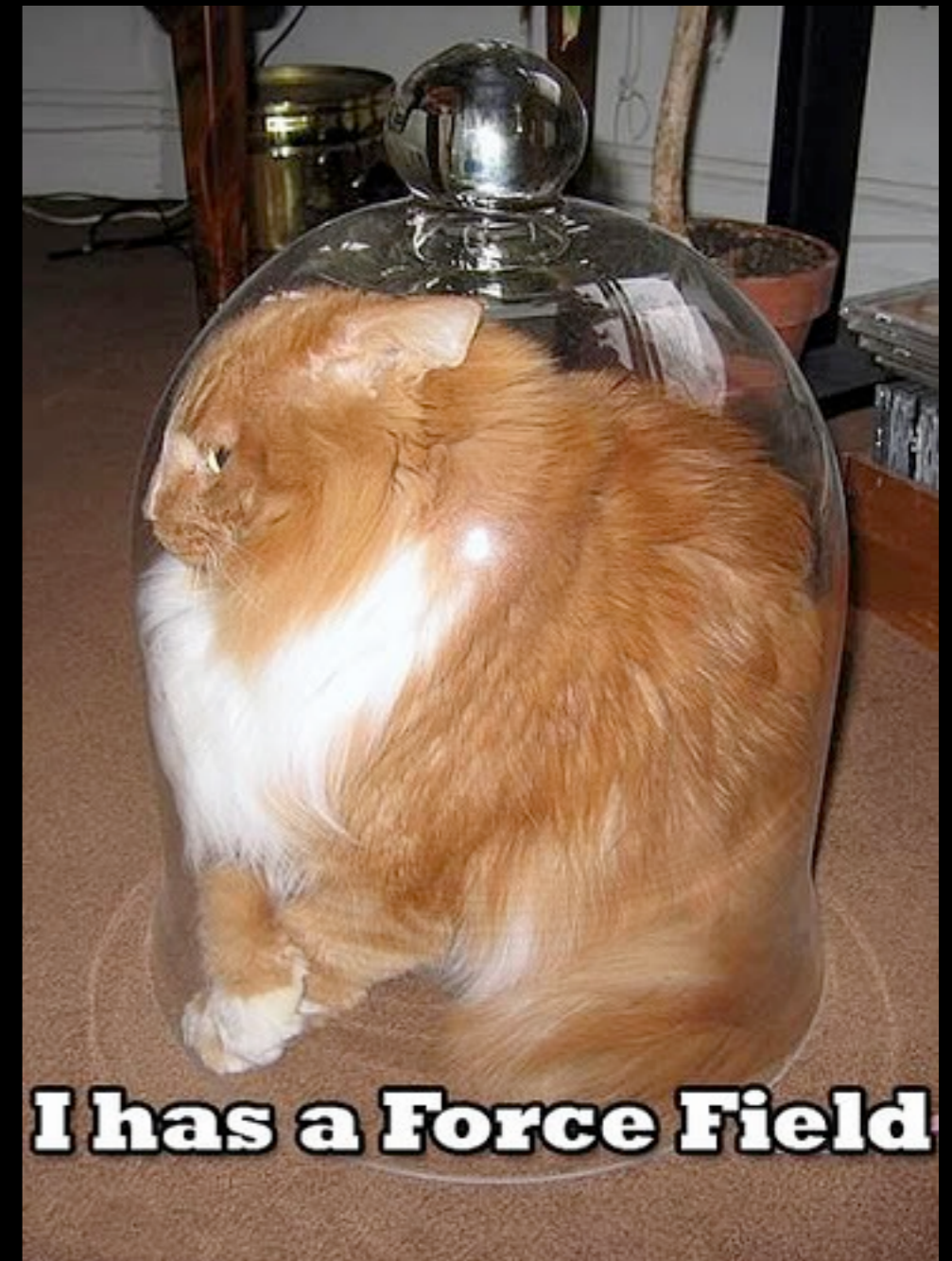
05 OCT 09 [RFID Card Reader USB](#) SAVE

[USB-RS232-PCB Converter](#) SAVE



Some more secrets

- Yes, all of the badge numbers were sequential.
 - You had the right to know who has access to your system!
 - This would have given you all of the sequential IDs and that of the admin for the system...
- How often do you think that vendors use the same authentication (user/password, etc) across multiple customers?
- How often do you think that vendors make the same mistakes across multiple clients?
 - Yes, red team badges were sequential too
 - There was some separation between both, but brute force was possible in a few minutes....



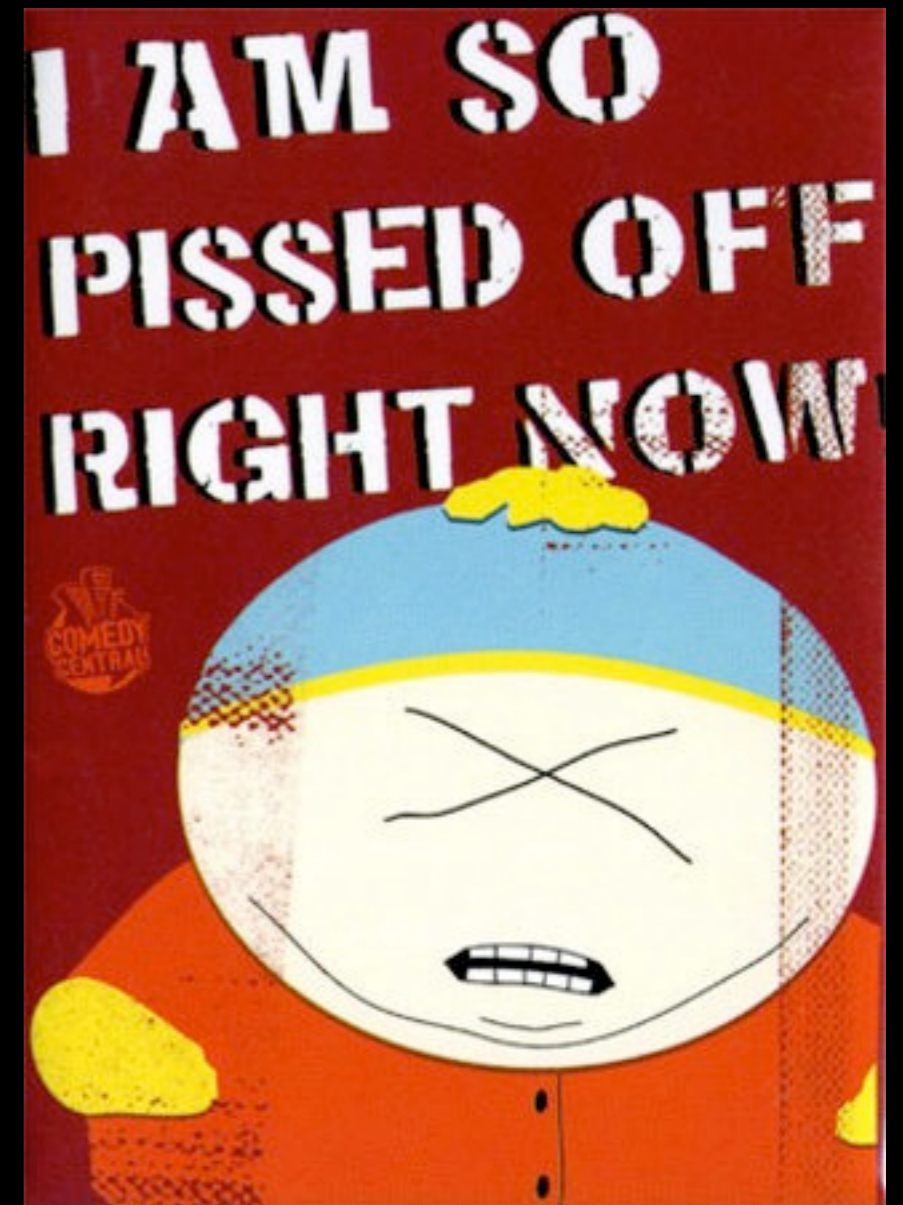
Some more secrets

- Speaking of doing stupid things, this vendor did something stupid too...
 - That red team hack? Yeah, it is mostly my fault and probably something you all learned too.
 - I'll let Paul talk about this during his debrief!
- You'll also note that the vendor did not disclose the exposure...
 - Did the vendor break the law?
 - What do you think might happen if the truth came out?



Some more secrets

- It is bad to piss off your vendor(s)
 - Bad mouthing your vendors is never a good idea, especially when it gets back to them
 - Depending on where you say it or who you say it to can bet you sued. That's called defamation (if it isn't true).
 - In this case, the vendor elected not to renew the support contract



Some more secrets

- It is also extremely bad to piss off the hackers...
 - They do bad things to you..
 - I know, they have been already
 - But it could be worse, such as mass infiltration
 - Rickrolling
 - Or sending in this guy...



Some more secrets



So Long and Thanks For All of the Fish!

- I hope you enjoyed the fun!
- Hopefully we gave you somethings to think about in the “real world”
- Got suggestions for improvements or additions? Questions? I’d love to hear them!

larry@pauldotcom.com

