# Let’s Open our Security Practices

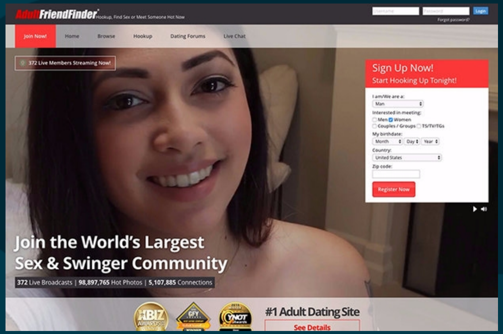
Greg Scott – gscott@redhat.com
CISSP number 358671

PLEASE GO ONLINE OR CALL
FROM YOUR HOME PHONE TO
ACTIVATE YOUR CARD

www.bankofamerica.com/activate
1.800.276.9939

# Agenda

- What’s wrong with security today?
- What’s the cure?
- Have I lost my mind?
- Call to action.



372 Live Members Streaming Now!

Sign Up Now!
Start Hooking Up Tonight!

I am/We are a: Man

Interested in meeting:
☐ Men ☑ Women
☐ Couples / Groups ☐ TS/TV/TGs

My birthdate: Month Day Year

Country: United States

Zip code:

Join the World's Largest Sex & Swinger Community

372 Live Broadcasts | 98,897,765 Hot Photos | 5,107,885 Connections

#1 Adult Dating Site

# 1.34 billion records leaked in April 2019 cyberattacks

From https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-april-2019-1-34-billion-records-leaked

- Criminal accesses personal data of faculty staff and students at Georgia Tech(1.3 million)
- Bangladesh Oil, Gas and Mineral Corporation’s website hacked hours after recovering from previous attack (unknown)
- Australian Signals Directorate confirms data was stolen in parliament IT breach(unknown)
- Massachusetts hospital caught in phishing scam (12,000)
- Hacker breached Minnesota state agency email (11,000)
- South Carolina’s Palmetto Health discloses phishing attack dating back to 2018(23,811)
- Phishing scam exposes personal data at Florida’s Clearway Pain Solutions Institute (35,000)
- Customer data stolen as website of Japanese luxury railway hit by cyber attack(8,000)
- Dakota County, MN, discloses breach after an employee’s email is hacked(1,000)
- Blue Cross of Idaho notifies members of privacy breach after thwarting financial fraud (5,600)
- Texas’s Questcare Medical Services investigating business email compromise attack (unknown)
- Ontario’s Stratford City Hall recovers from cyber attack (unknown)
- IT outsourcing and consulting giant Wipro hacked (unknown)
- Texas-based Metrocare Services discloses second breach in five months (5,290)

# More cyberattacks

- California-based Centrelake Medical Group notifies patients of security incident(unknown)
- North Carolina’s Klaussner Furniture Industries notifies employees of security incident (9,352)
- Customers at US fast food retailer Chipotle say their accounts have been hacked (unknown)
- Minnesota’s Riverplace Counseling Center notifies patients after malware infection (11,639)
- Hacktivists attack UK police sites to protest arrest of Julian Assange (unknown)
- Texas-based EmCare says patient and employee data has been hacked (60,000)
- Idaho-based bodybuilding.com discloses employee-related data breach(unknown)
- Illinois dental insurer notifies members after phishing attack (unknown)
- Attackers breached Docker Hub, grabbed keys and tokens (190,000)
- Atlanta’s Woodruff Arts Center shuts down network amid security breach(unknown)
- University of Alaska discloses data breach that occurred more than a year ago(unknown)
- Magecart hackers steal data from Atlanta Hawks’ online shop (unknown)

# Ransomware

- Genesee County, MI, government suffers 'aggressive' ransomware attack(unknown)
- Ransomware attack affects Women's Health Care Group of PA (300,000)
- Greenville, NC, government's systems knocked out by ransomware (unknown)
- Ransomware attack hits Garfield County, UT (unknown)
- Augusta, ME, hit by ransomware, forcing City Center to close (unknown)
- New Jersey-based paediatric orthopaedic surgeon hit by ransomware (unknown)
- Ransomware at Florida's Stuart City Hall "more than likely" caused by phishing(unknown)
- Massachusetts-based medical billing services notifies patients of ransomware attack (unknown)
- Idaho's Sugar-Salem School District 322 hit by ransomware during ISAT testing(unknown)
- Ransomware disables Cleveland airport's email systems, information screens(unknown)

# Data breaches

- Indian government leaves healthcare database exposed on web (12.5 million)
- West Yorkshire council data leak leaves couple who adopted abused children living in fear (2)
- History repeats itself as Facebook third-party apps expose users’ personal data(540 million)
- Canadian pension firm loses microfiche containing personal data (unknown)
- Crook swipes Winnipeg Regional Health Authority employee’s bag; patients’ records taken (75)
- VoterVoice exposes database containing ‘treasure trove’ of personal data(300,000)
- Ohio government accidentally leaks information of those seeking job, family services and health aid (993)
- Chinese companies responsible for massive data breach of CVs (590 million)
- Texas’s Weslaco Regional Rehabilitation Hospital discloses data breach(unknown)
- Russian hospital dumps medical waste, sensitive data in landfill site (unknown)
- UK’s Home Office sorry for EU citizen data breach (240)
- Pennsylvania’s Community College of Allegheny County discloses data breach(unknown)
- Patients at Toledo, OH, rehab hospital subject to data breach (unknown)

# More data breaches

- Washington state-based RS Medical discloses incident that may have compromised patient information (unknown)
- Athens, OH, rehabilitation centre notifies patients after unauthorised access to network (20,485)
- Sensitive data found on hard disks may be India’s largest ever data breach (78 million)
- California-based LD Evans says it has only just learned about 2018’s Citrix vulnerability (631)
- India’s JustDial service is breaching users’ personal data in real time (100 million)
- Drug addicts’ personal data found in rehab centres’ unexposed databases (4.91 million)
- Researcher uncovers exposed personal data from Iranian ride-hailing app(6,772,269)
- Pennsylvania-based Partners for Quality discloses data breach (3,673)
- US health provider Inmediata discovers patients’ information was exposed on the web (unknown)
- ‘Horrendous’ privacy breach at Australia’s Centrelink sees clients’ names published on Facebook (unknown)
- Personal data of employees at Lauderdale County, MS, emailed to colleagues(100)
- US consumer commission warns of data breach affecting safety information(unknown)

# Financial information

- Almost $500,000 swiped in Tallahassee, FL, payroll hack (unknown)
- AeroGrow says hackers stole months of credit card data (unknown)
- Florida-based United Way of the Big Bend says tax payers’ info was sto len (64)
- KPMG faces fine of up to $1.6 million after leaking payroll data (41)

# Malicious insiders and miscellaneous incidents

- Former IT aide to New Hampshire senator caught keylogging (unknown)
- Employee at Cleveland’s University Hospital accidentally shared patients’ health info
  (840)
- University of Toledo counsellor fired after allegedly disclosing a student’s PTSD(1)
- Maine’s Acadia Hospital mistakenly release confidential information of Suboxone patients
  (300)
- Employee at California’s St. Boniface Hospital “inappropriately” viewed patient records
  (38)

# In other news...

- USB stick containing sensitive data (and the movie *Gone Girl*) *discovered during manslaughter trial* (6,385)
- Barking resident jailed for blackmailing porn watchers (unknown)
- Source code of Iranian cyber-espionage tools leaked on Telegram (unknown)
- Supply chain hackers snuck malware into video games (unknown)

# I counted 74 data leakage stories in April, 2019

- 74 data leakage incidents
- 30 days in April
- Average of 2.47 per day

On average, every day in April saw about 2 ½ data leakage incidents.

That’s what was documented.

# One more data point

The US Dept. of Homeland Security says we endure 4000 ransomware attacks ***every day.***

Link the ProPublica article below

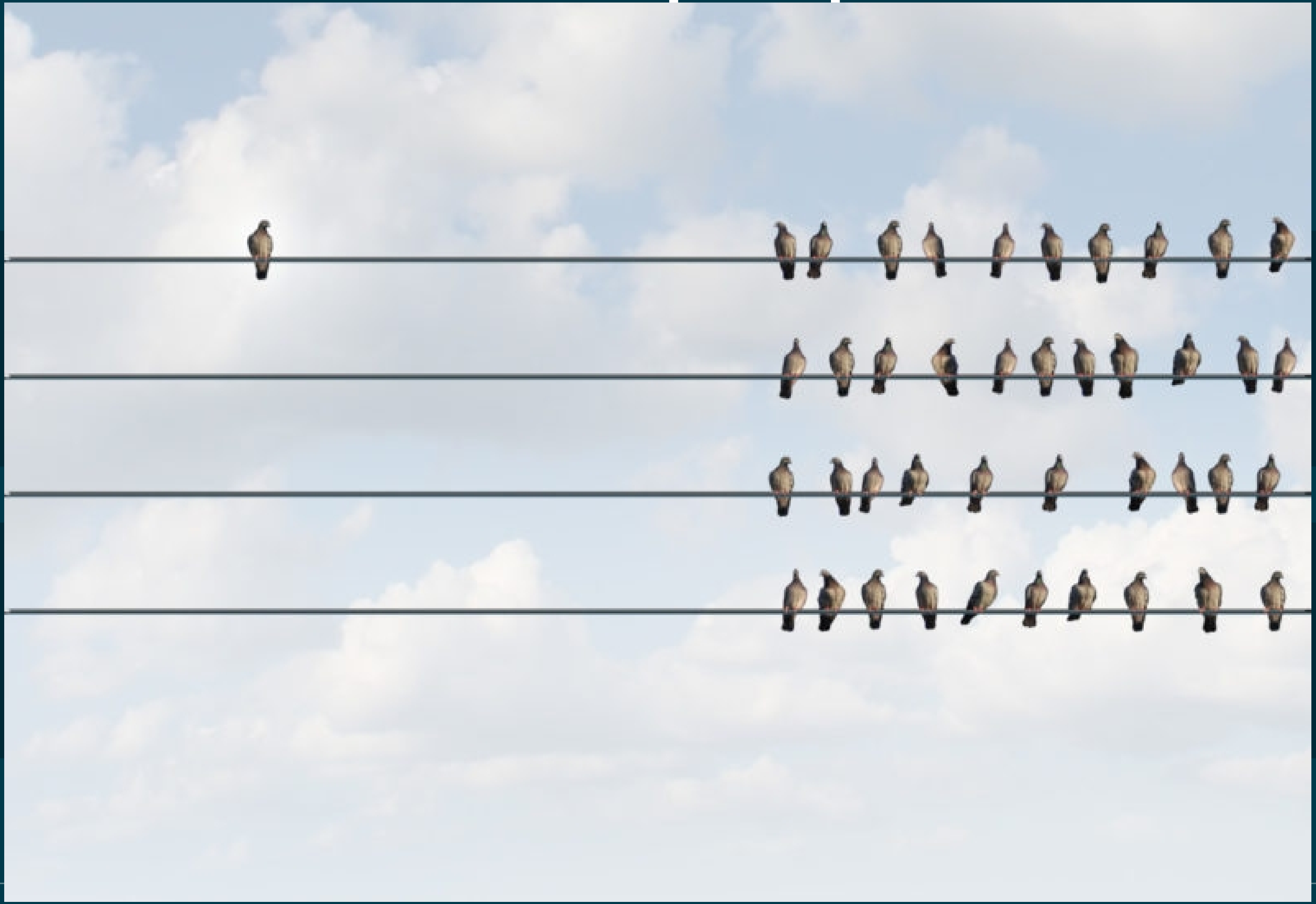
https://features.propublica.org/ransomware/ransomware-attack-data-recovery-firms-paying-hackers/

# What do all these attacks have in common?

- For nearly all, we don’t know what went wrong and what they did to fix it.
- Except for Equifax, but that took a Congressional investigation.
- Here is a SANS article with a link to the Equifax report: https://www.sans.org/security-awareness-training/blog/just-released-congressional-report-equifax-hack

# What’s the cure?

# A counter-intuitive proposal



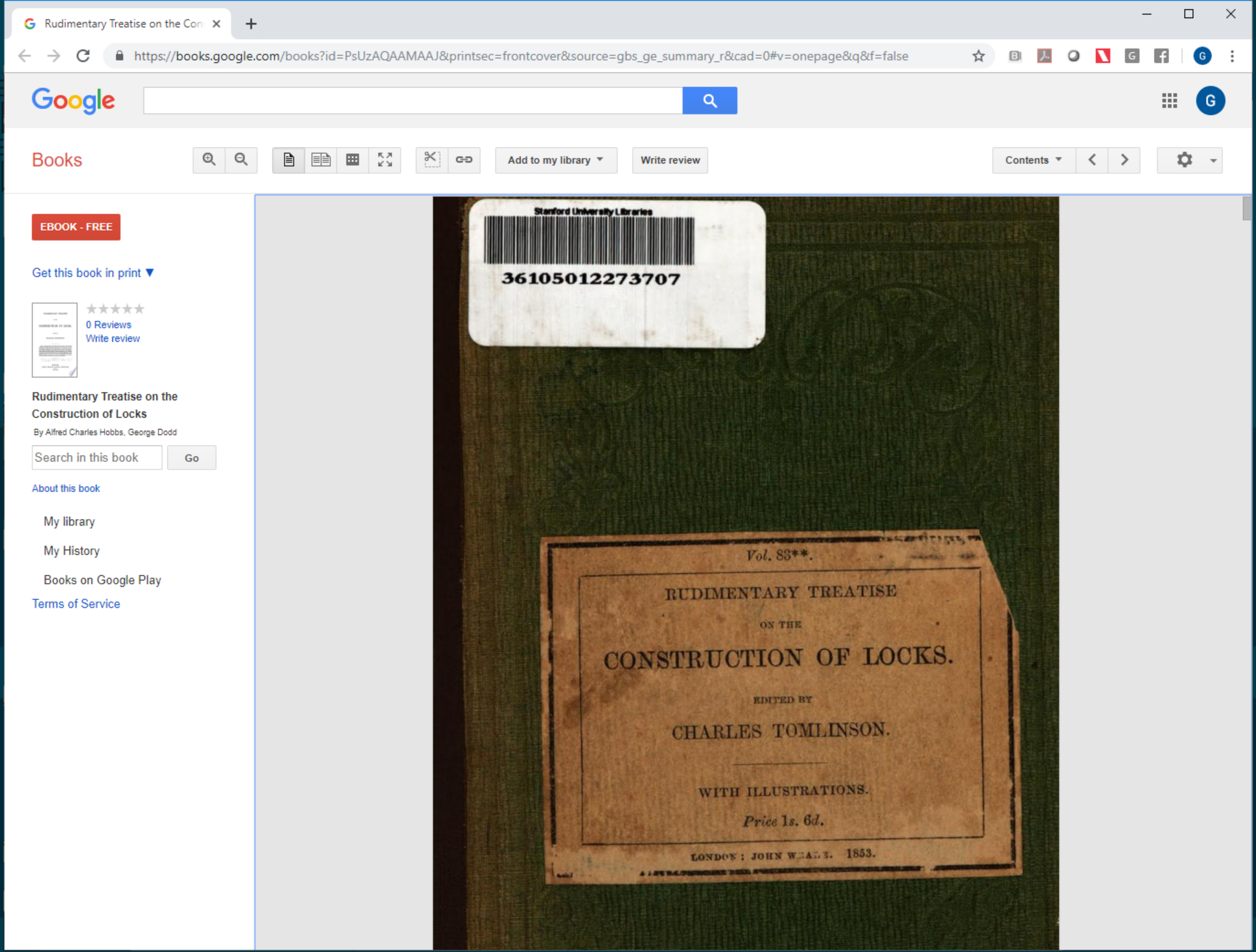
# Open it all up

- Internal topology
- Permission model
- Incident response plan
- Post-mortems
- Write articles about our security practices.
- Present them at conferences.
  - Accept peer review criticism.
  - Critique others.
  - Game out scenarios with other organizations.

Demand openness from your suppliers.

Provide openness to your stakeholders.

# Have I lost my mind?


Rudimentary Treatise on the Con
https://books.google.com/books?id=PsUzAQAAMAAJ&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false
Google
Books
Add to my library
Write review
Contents
EBOOK - FREE
Get this book in print ▼
0 Reviews
Write review

Rudimentary Treatise on the Construction of Locks

By Alfred Charles Hobbs, George Dodd

Vol. 83**.

RUDIMENTARY TREATISE
ON THE
CONSTRUCTION OF LOCKS.
EDITED BY
CHARLES TOMLINSON.

WITH ILLUSTRATIONS.
*Price* 1s. 6d.

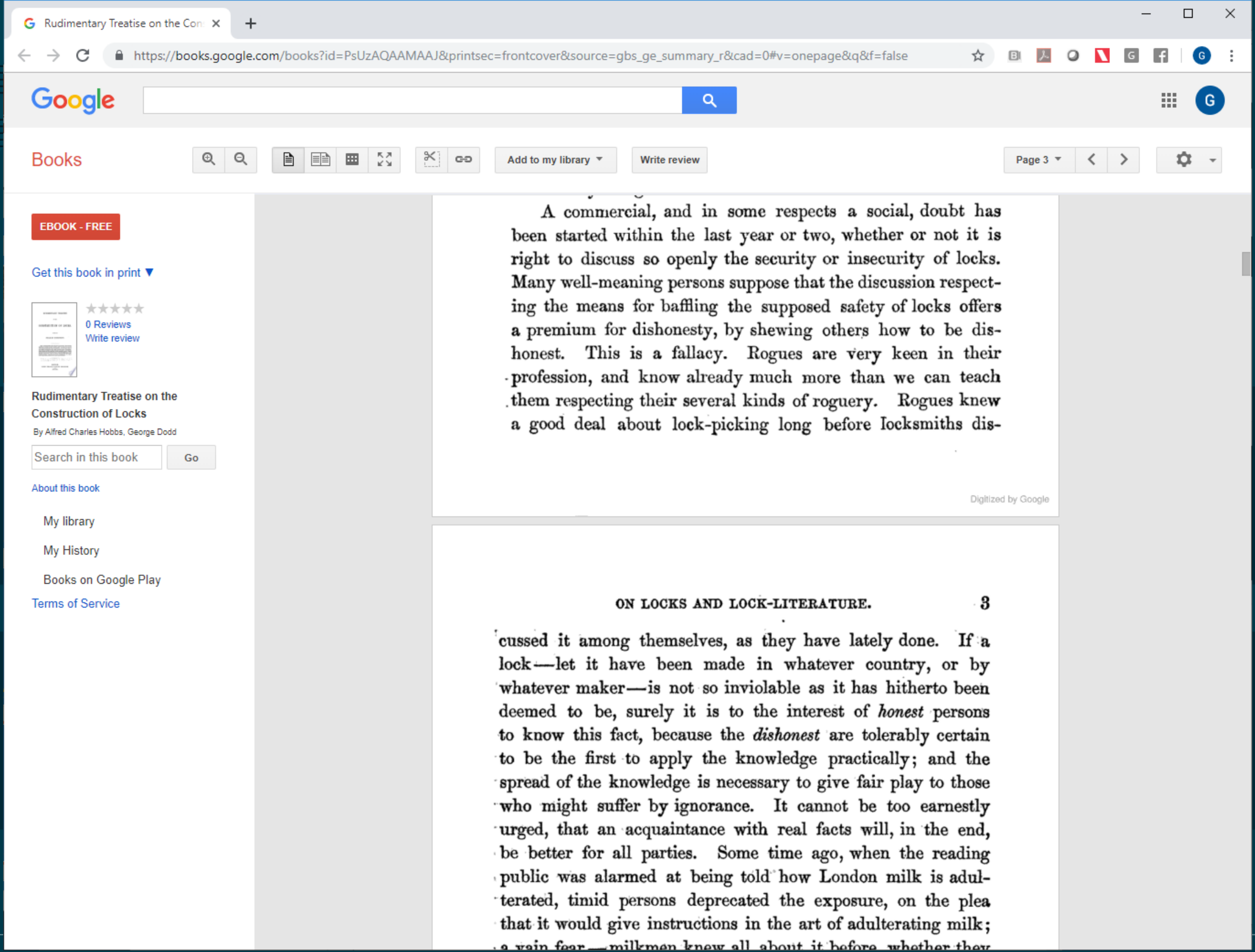
LONDON: JOHN WEALE. 1853.

Rudimentary Treatise on the Construction of Locks

Edited by Charles Tomlinson and Alfred Charles Hobbs

John Weale, High Holborn, 1853

https://books.google.com/books?id=PsUzAQAAMAAJ&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false


Rudimentary Treatise on the Con
https://books.google.com/books?id=PsUzAQAAMAAJ&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false
Google
Books
Add to my library
Write review
Page 3
EBOOK - FREE
Get this book in print ▼
0 Reviews
Write review
Rudimentary Treatise on the Construction of Locks
By Alfred Charles Hobbs, George Dodd
Search in this book
Go
About this book
My library
My History
Books on Google Play
Terms of Service
Digitized by Google

A commercial, and in some respects a social, doubt has been started within the last year or two, whether or not it is right to discuss so openly the security or insecurity of locks. Many well-meaning persons suppose that the discussion respecting the means for baffling the supposed safety of locks offers a premium for dishonesty, by shewing others how to be dishonest. This is a fallacy. Rogues are very keen in their profession, and know already much more than we can teach them respecting their several kinds of roguery. Rogues knew a good deal about lock-picking long before locksmiths dis-

ON LOCKS AND LOCK-LITERATURE. 3

cussed it among themselves, as they have lately done. If a lock—let it have been made in whatever country, or by whatever maker—is not so inviolable as it has hitherto been deemed to be, surely it is to the interest of *honest* persons to know this fact, because the *dishonest* are tolerably certain to be the first to apply the knowledge practically; and the spread of the knowledge is necessary to give fair play to those who might suffer by ignorance. It cannot be too earnestly urged, that an acquaintance with real facts will, in the end, be better for all parties. Some time ago, when the reading public was alarmed at being told how London milk is adulterated, timid persons deprecated the exposure, on the plea that it would give instructions in the art of adulterating milk; a vain fear—milkmen knew all about it before, whether they

Bottom of page 2, top of page 3

# Paragraph breaks and color added for readability

A commercial, and in some respects a social, doubt has been started within the last year or two, whether or not it is right to discuss so openly the security or insecurity of locks. Many well-meaning persons suppose that the discussion respecting the means for baffling the supposed safety of locks offers a premium for dishonesty, by shewing others how to be dishonest.

This is a fallacy.

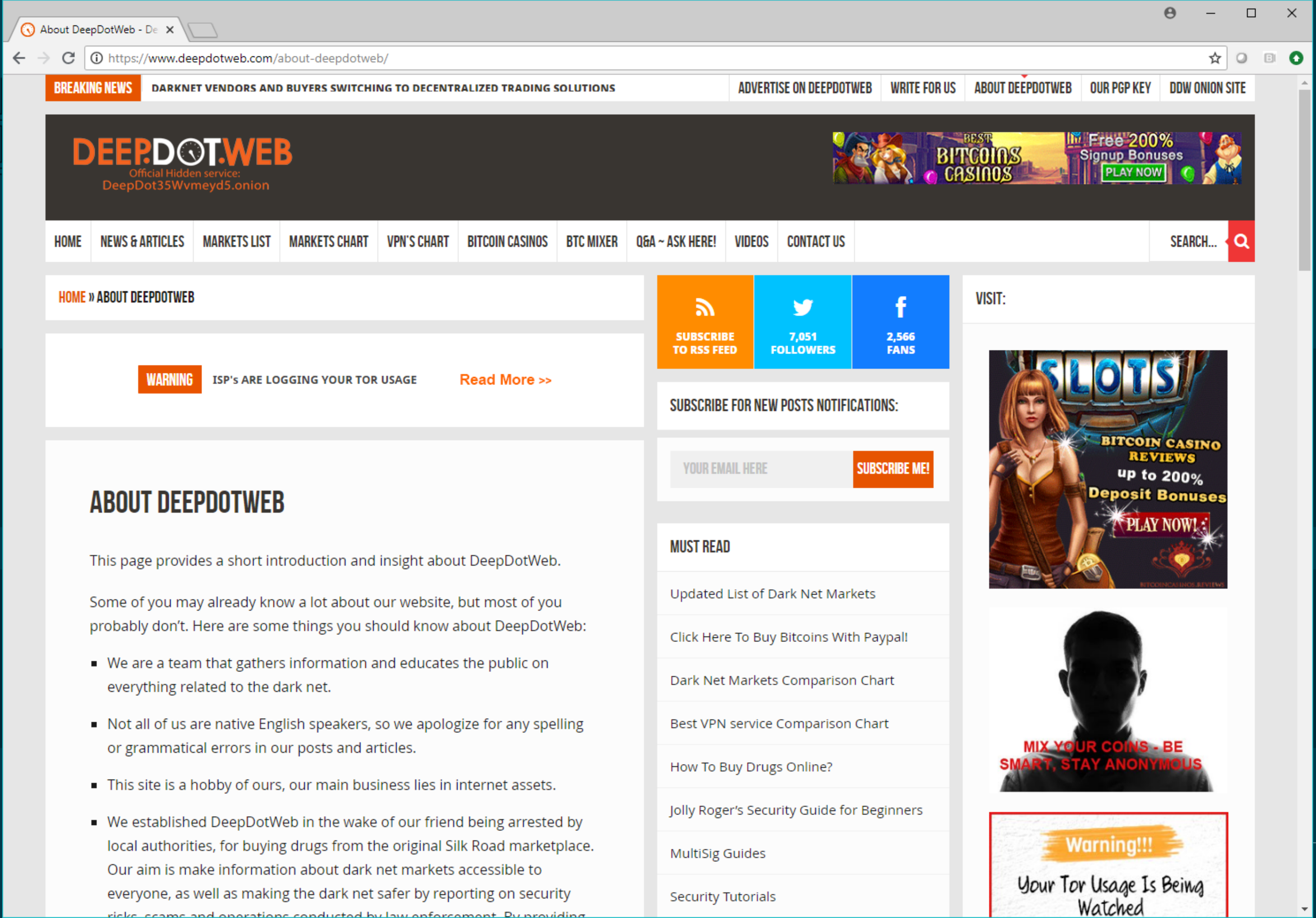
Rogues are Very keen in their profession, and know already much more than we can teach them respecting their several kinds of roguery. Rogues knew a good deal about lock-picking long before locksmiths discussed it among themselves, as they have lately done.

If a lock—let it have been made in whatever country, or by whatever maker—is not so inviolable as it has hitherto been deemed to be, surely it is to the interest of honest persons to know this fact, because the dishonest are tolerably certain to be the first to apply the knowledge practically; and the spread of the knowledge is necessary to give fair play to those ‘who might suffer by ignorance.

It cannot be too earnestly urged, that an acquaintance with real facts will, in the end, be better for all parties.

# 2019 language

- Bad guys spend all day probing good guys.
  - And all night collaborating with each other to improve the next day’s probes.
- Bad guys already know relevant details about our internal networks.
- Good guys isolate ourselves.
- We need to level the playing field.



## ABOUT DEEPDOTWEB

This page provides a short introduction and insight about DeepDotWeb.

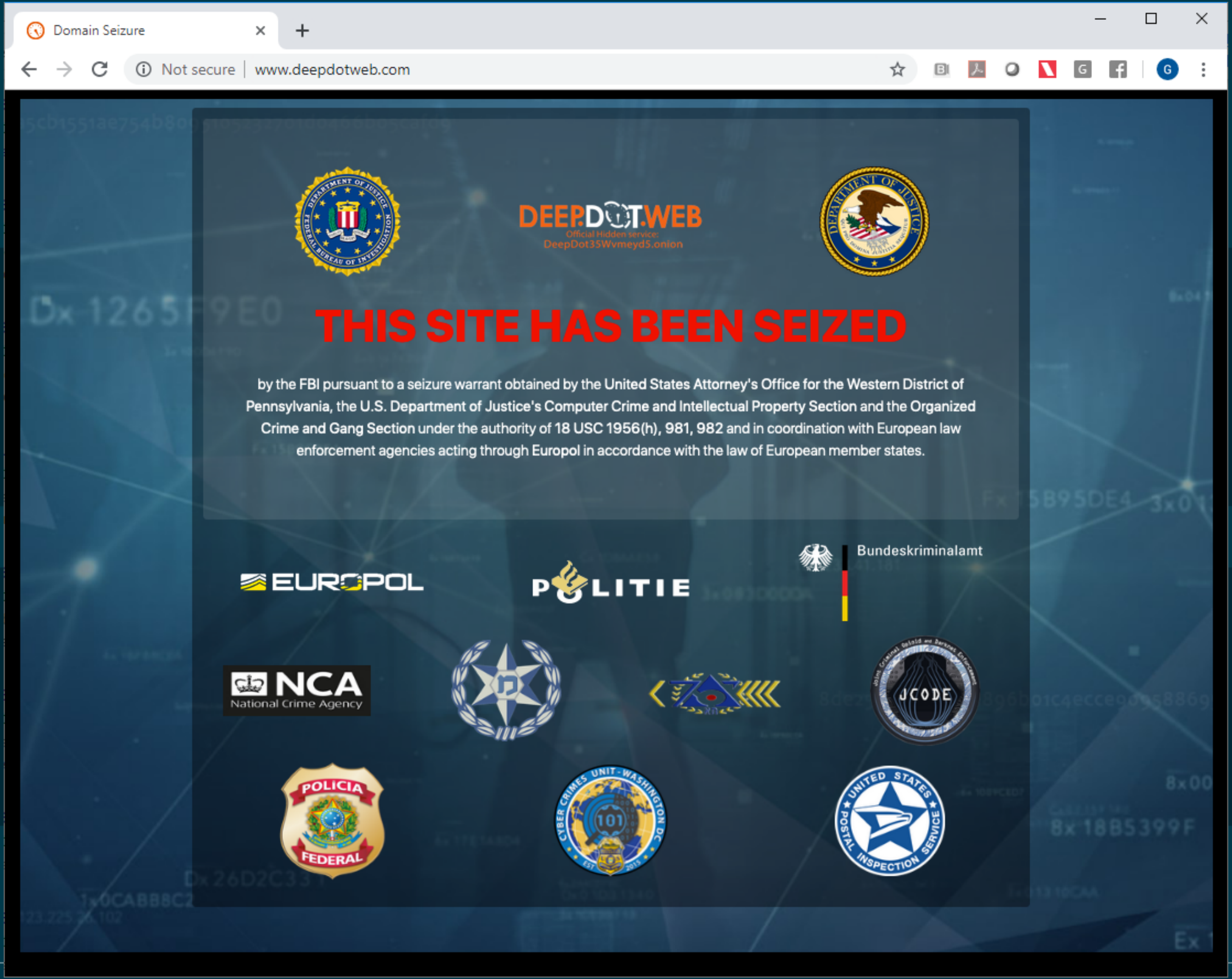
Some of you may already know a lot about our website, but most of you probably don't. Here are some things you should know about DeepDotWeb:

- We are a team that gathers information and educates the public on everything related to the dark net.
- Not all of us are native English speakers, so we apologize for any spelling or grammatical errors in our posts and articles.
- This site is a hobby of ours, our main business lies in internet assets.
- We established DeepDotWeb in the wake of our friend being arrested by local authorities, for buying drugs from the original Silk Road marketplace. Our aim is make information about dark net markets accessible to everyone, as well as making the dark net safer by reporting on security risks, scams and operations conducted by law enforcement. By providing

How do bad guys win?

They collaborate.

# Good guys also win by collaborating



Domain Seizure

Not secure | www.deepdotweb.com

DEEPDOTWEB
Official Hidden service:
DeepDot35Wvmeyd5.onion

THIS SITE HAS BEEN SEIZED

by the FBI pursuant to a seizure warrant obtained by the United States Attorney's Office for the Western District of Pennsylvania, the U.S. Department of Justice's Computer Crime and Intellectual Property Section and the Organized Crime and Gang Section under the authority of 18 USC 1956(h), 981, 982 and in coordination with European law enforcement agencies acting through Europol in accordance with the law of European member states.

Check out this article from Wired Magazine:

[https://www.wired.com/story/dark-web-drug-takedowns-deepdotweb-rebound/](https://www.wired.com/story/dark-web-drug-takedowns-deepdotweb-rebound/)

Score one for the good guys.

# I’m just a sysadmin; nobody listens to me!

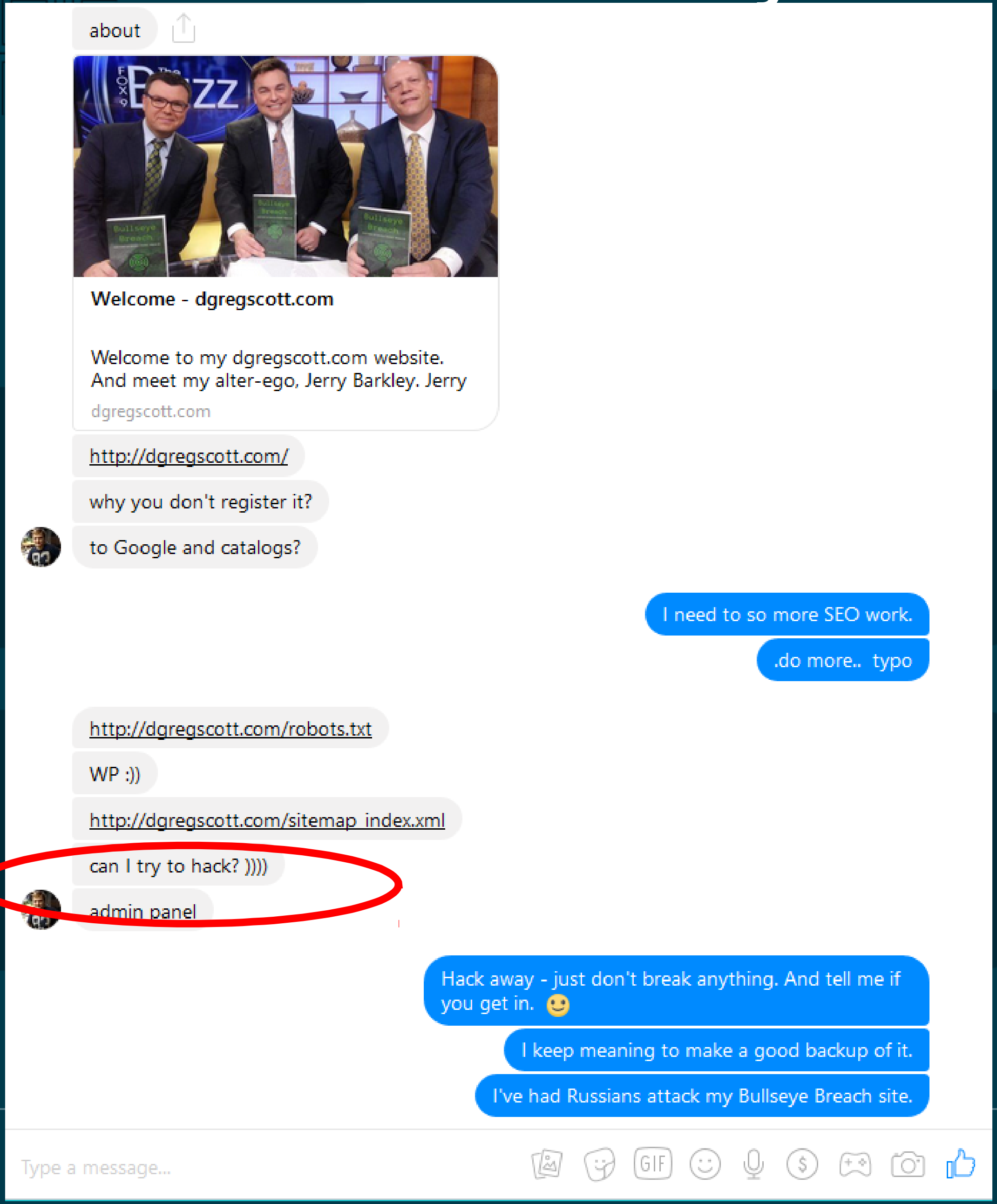
# Well then, listen to guys like Warren Buffet.

"I don't know that much about cyber, but I do think that's the number one problem with mankind." –Warren Buffet

From https://www.businessinsider.com/warren-buffett-cybersecurity-berkshire-hathaway-meeting-2017-5

# Taking my own medicine

# My buddy, Ihor



about

Welcome - dgregscott.com

Welcome to my dgregscott.com website. And meet my alter-ego, Jerry Barkley. Jerry

dgregscott.com

http://dgregscott.com/

why you don't register it?

to Google and catalogs?

I need to so more SEO work.

.do more.. typo

http://dgregscott.com/robots.txt

WP :))

http://dgregscott.com/sitemap_index.xml

can I try to hack? ))))

admin panel

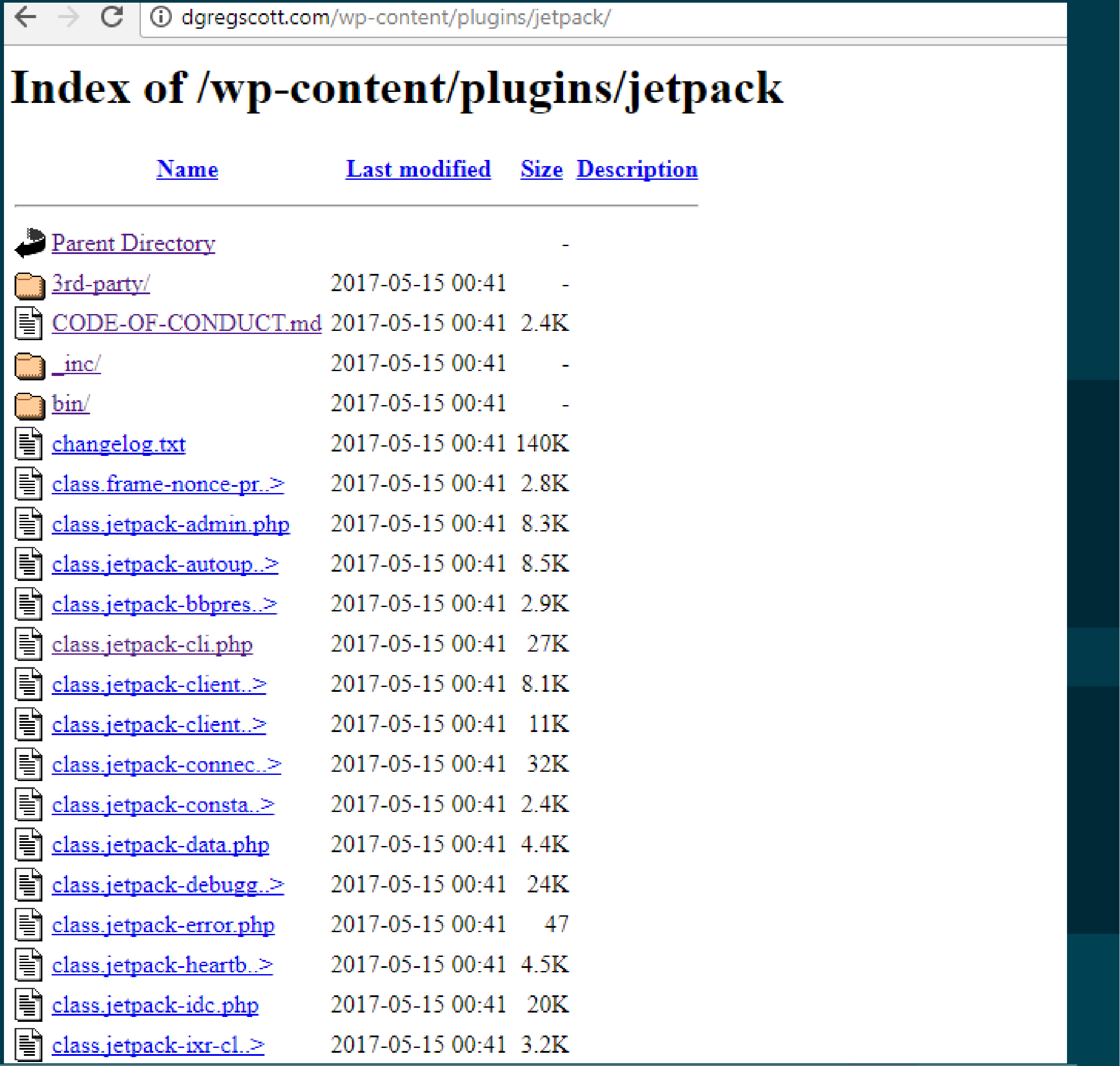
Hack away - just don't break anything. And tell me if you get in. 🙂

I keep meaning to make a good backup of it.

I've had Russians attack my Bullseye Breach site.

# http://dgregscott.com

Greg )
Man
Why? )))
come on ))))))))))
I think that’s only the beginning )))))))))
no no ))))))))))))))))
Greg ))



dgregscott.com/wp-content/plugins/jetpack/

# Index of /wp-content/plugins/jetpack

| Name | Last modified | Size | Description |
|---|---|---|---|
| Parent Directory | | - | |
| 3rd-party/ | 2017-05-15 00:41 | - | |
| CODE-OF-CONDUCT.md | 2017-05-15 00:41 | 2.4K | |
| _inc/ | 2017-05-15 00:41 | - | |
| bin/ | 2017-05-15 00:41 | - | |
| changelog.txt | 2017-05-15 00:41 | 140K | |
| class.frame-nonce-pr..> | 2017-05-15 00:41 | 2.8K | |
| class.jetpack-admin.php | 2017-05-15 00:41 | 8.3K | |
| class.jetpack-autoup..> | 2017-05-15 00:41 | 8.5K | |
| class.jetpack-bbpres..> | 2017-05-15 00:41 | 2.9K | |
| class.jetpack-cli.php | 2017-05-15 00:41 | 27K | |
| class.jetpack-client..> | 2017-05-15 00:41 | 8.1K | |
| class.jetpack-client..> | 2017-05-15 00:41 | 11K | |
| class.jetpack-connec..> | 2017-05-15 00:41 | 32K | |
| class.jetpack-consta..> | 2017-05-15 00:41 | 2.4K | |
| class.jetpack-data.php | 2017-05-15 00:41 | 4.4K | |
| class.jetpack-debugg..> | 2017-05-15 00:41 | 24K | |
| class.jetpack-error.php | 2017-05-15 00:41 | 47 | |
| class.jetpack-heartb..> | 2017-05-15 00:41 | 4.5K | |
| class.jetpack-idc.php | 2017-05-15 00:41 | 20K | |
| class.jetpack-ixr-cl..> | 2017-05-15 00:41 | 3.2K | |

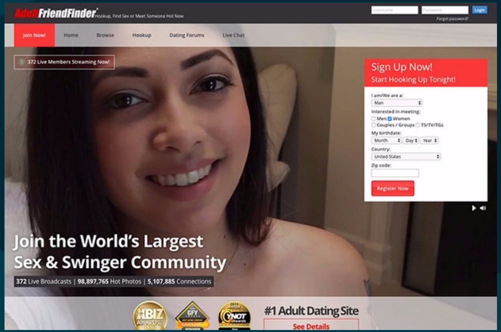
# The cure

I used a different directory on this Wordpress website than normal and the default settings could have killed me.

```
<Directory /var/www/html/wordpress>

##  Options Indexes FollowSymLinks
# Get rid of Indexes to prohibit directory searches

    Options FollowSymLinks
.
.
.
</Directory>
```


AdultFriendFinder Hookup, Find Sex or Meet Someone Hot Now

Forgot password?

Join Now! Home Browse Hookup Dating Forums Live Chat

372 Live Members Streaming Now!

Sign Up Now!
Start Hooking Up Tonight!

I am/We are a:
Man

Interested in meeting:
□ Men ☑ Women
□ Couples / Groups □ TS/TV/TGs

My birthdate:
Month Day Year

Country:
United States

Zip code:

Register Now

Join the World's Largest
Sex & Swinger Community

372 Live Broadcasts | 98,897,765 Hot Photos | 5,107,885 Connections

#1 Adult Dating Site
See Details

# What if these organizations were open?

- Equifax may have saved more than $1 billion in remediation costs.
- Uber would not have become an unwitting partner with people who stole from it.
- Ransomware attacks might not have disrupted Atlanta, Baltimore, and more than twenty other cities recently.
- (Your organization here)

# Contact info

Greg Scott

gscott@redhat.com

http://www.dgregscott.com

Twitter: DGregScott

LinkedIn: https://www.linkedin.com/in/dgregscott/

Youtube: “Greg Scott Public Videos” at https://www.youtube.com/channel/UCBtDWsqzMZ_RB94I_F4cnRQ