Let’s Open our Security Practices

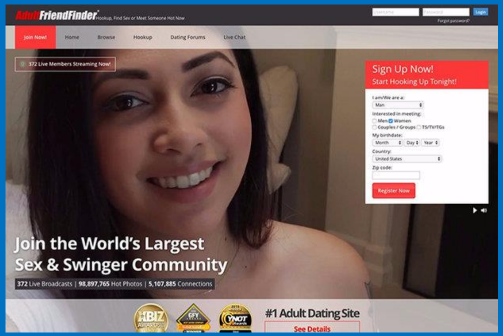
—D. Greg Scott—

CISSP Number 358671

DISCOVER
Cashback Bonus
Bank of America
PLEASE GO ONLINE OR CALL FROM YOUR HOME PHONE TO ACTIVATE YOUR CARD
www.bankofamerica.com/activate
1.800.276.9939
BANKAMERICARD
DANIEL GREGORY SCOTT
THE HOME DEPOT
COMMERCIAL REVOLVING CHARGE
DISCOVER
Cashback Bonus
amazon
VISA

Agenda

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


AdultFriendFinder Hookup, Find Sex or Meet Someone Hot Now

Username Password Login
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

66 million records breached in 95 attacks in the news in Jan. 2022

From https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-january-2022-66-million-records-breached

Cyber attacks

- **Gloucester Council cyber attack linked to Russian hackers** (unknown)
- **Parents warned after scam emails at Liverpool secondary school** (unknown)
- DatPiff data being sold online after password-cracking attack (7.5 million)
- New York Attorney General alerts companies to credential-stuffing cyber attacks (1.1 million)
- Jefferson Surgical Clinic notifies those affected by 2021 data breach (174,769)

More Cyber Attacks

- Singapore-based department store OG suffers security incident (unknown)
- Indonesian govt responds to massive data leak of medical records (6 million)
- Monroe Public Schools notifies those affected by malware attack (1,201)
- Data captured from Siriraj Hospital put up for sale on dark web (39 million)
- Visalia Unified School District notifying employees and students about security incident (35,000)
- Hackers raided Panasonic server for months, stealing personal data of job seekers (unknown)
- Memorial Health System notifies patients of malware incident (216,478)
- Canadian city of Brantford says its city hall has been breached (unknown)
- Cyber attack hits Ukrainian websites as Russia tensions mount (unknown)
- City of Tenino loses $280,309 to phishing email scam (unknown)

Still More Cyber Attacks

- Data stolen in attack at Arnprior Regional Health (unknown)
- Another hack on Lympo, lost 165.2 million LMT tokens (unknown)
- Red Cross discloses cyber attack affecting “highly vulnerable people” (515,000)
- Thousands of Indians’ Covid-19 related data leaked online (20,000)
- Anne Arundel Medical Center discloses phishing attack (unknown)
- Peachtree Orthopaedic Clinic reports breach to HHS (53,686)
- Sacramento County employee fell for phishing scam (2,096)
- Brazil’s Acesso Soluções de Pagamento suffers cyber attack (160,100)
- Patient info possibly disclosed in Spokane Health District phishing attack (1,000)
- Canada’s Foreign Affairs Ministry hacked (unknown)

A Few More Cyber Attacks

- Pennsbury School District's computer system breached (unknown)
- North Korean Internet downed by DDoS attacks (unknown)
- NHS Management discloses incident from last May (unknown)
- Nobel Foundation site hit by DDoS attack on award day (unknown)
- Mall retailer Spencer Gifts discloses cyber attack (unknown)
- True Health New Mexico says it was targeted by cyber attack (62,000)
- StarTek says it was hit by cyber attack (unknown)
- Taylor Regional Hospital phone lines still down after reported cyber attack (unknown)

Ransomware Attacks

- Attack on FinalSite shuts down thousands of school websites (unknown)
- Missouri school district's employee data dumped by ransomware group (unknown)
- Maryland Department of Health confirms ransomware attack caused disruption in COVID-19 data last month (unknown)
- Portuguese newspaper Expresso hit by cyber criminals (unknown)
- Ransomware puts New Mexico prison in lockdown (unknown)
- Neenah schools in Wisconsin investigating apparent cyber attack (unknown)
- Compton and Broomhead Dental Center alleged victim of cyber attack (unknown)
- Hospital Centro de Andalucia recovered quickly from ransomware attack (unknown)
- National Association of Community Health Centers to notify current and former employees of data breach (935)
- Guilford Technical Community College notifies those affected by ransomware (65,646)

More Ransomware

- Florida-based Jackson Hospital hit by ransomware (unknown)
- Albuquerque schools confirm ransomware attack, resume class (unknown)
- Italian fashion brand Moncler confirms ransomware attack and data breach (unknown)
- OpenSubtitles discloses successful extortion attempt (unknown)
- Griggsville-Perry School District hit by ransomware attack (unknown)
- Memorial Health System fell victim to ransomware (200,000)
- Valley Regional Transit target of ransomware attack (535)
- Charlotte YMCA alerts members of a security incident (unknown)
- Hacktivists attack Belarus railway intended to disrupt Russian forces (unknown)
- Midland University in Nebraska victim of ransomware attack last January (13,716)

A Few More Ransonware Attacks

- Conti ransomware hits Apple, Tesla supplier (unknown)
- Data from scheduling service FlexBooker stolen in cyber attack (10 million)
- Hospitality chain McMenamins releases notice after ransomware attack (unknown)
- Medical Healthcare Solutions now notifying clients' patients (unknown)
- Staffing firm ExecuSearch Holdings in suspected ransomware attack (42,000)
- Iowa-based Ottumwa dental office notifies patients of ransomware attack (26,144)
- Ransomware group threatens to leak data from France's justice ministry (9,859)

Data breaches

- **Black Country hospital trust suffers 'significant IT data loss'** (unknown)
- **COVID test data breach at Worcestershire school** (unknown)
- **Sensitive information leaked after data breach at Greensward Academy** (unknown)
- Vodafone accidentally sent a customer personal details of other accounts (18)
- Names of unvaccinated DDSB staff accidentally shared (400)
- COVID testing appointment scheduling service discovers data breach (unknown)
- South Africa's new traffic fine system exposed personal data (unknown)
- Data from Sea Mar Community Health Centers breach leaks onto web (688,000)
- NYU Langone notifies those affected by mailing vendor error (1,123)
- St. Lucie's County drug screening lab notifying patients after discovering misconfiguration of web portal (14,500)
- California public office admits Covid-19 healthcare data breach (unknown)

Financial information

- UScellular discloses data breach after billing system hack (405)
- Grass Valley discloses 2021 data breach (unknown)
- Major Indian fashion retailer hacked and data leaked (unknown)
- South Australian gov issues breach notice to hacked payroll provide (80,000)
- Hacker steals $200,000 through Multichain bug, offers to return 80% to victim (unknown)

Malicious insiders and miscellaneous incidents

- Ex-hospital worker arrested in SGMC data breach (unknown)
- Philippines govt says sacks of criminal records were stolen (unknown)
- University of Arkansas for Medical Sciences notifying patients after employee emailed PHI to her personal email account (518)
- US DoD staffer with top-secret clearance stole identities from work systems to apply for loans (37)

In other news…

- FTC warns companies to remediate Log4j security vulnerability
- A Missouri reporter is (still) getting blamed for the security flaw he exposed
- CEO of crypto exchange platform Cryptsy indicted for defrauding customers, destroying evidence, and tax evasion

95 Attacks Over 31 Days in January, 2022

Which averages to about 3 data leakage incidents that made the news every single day.

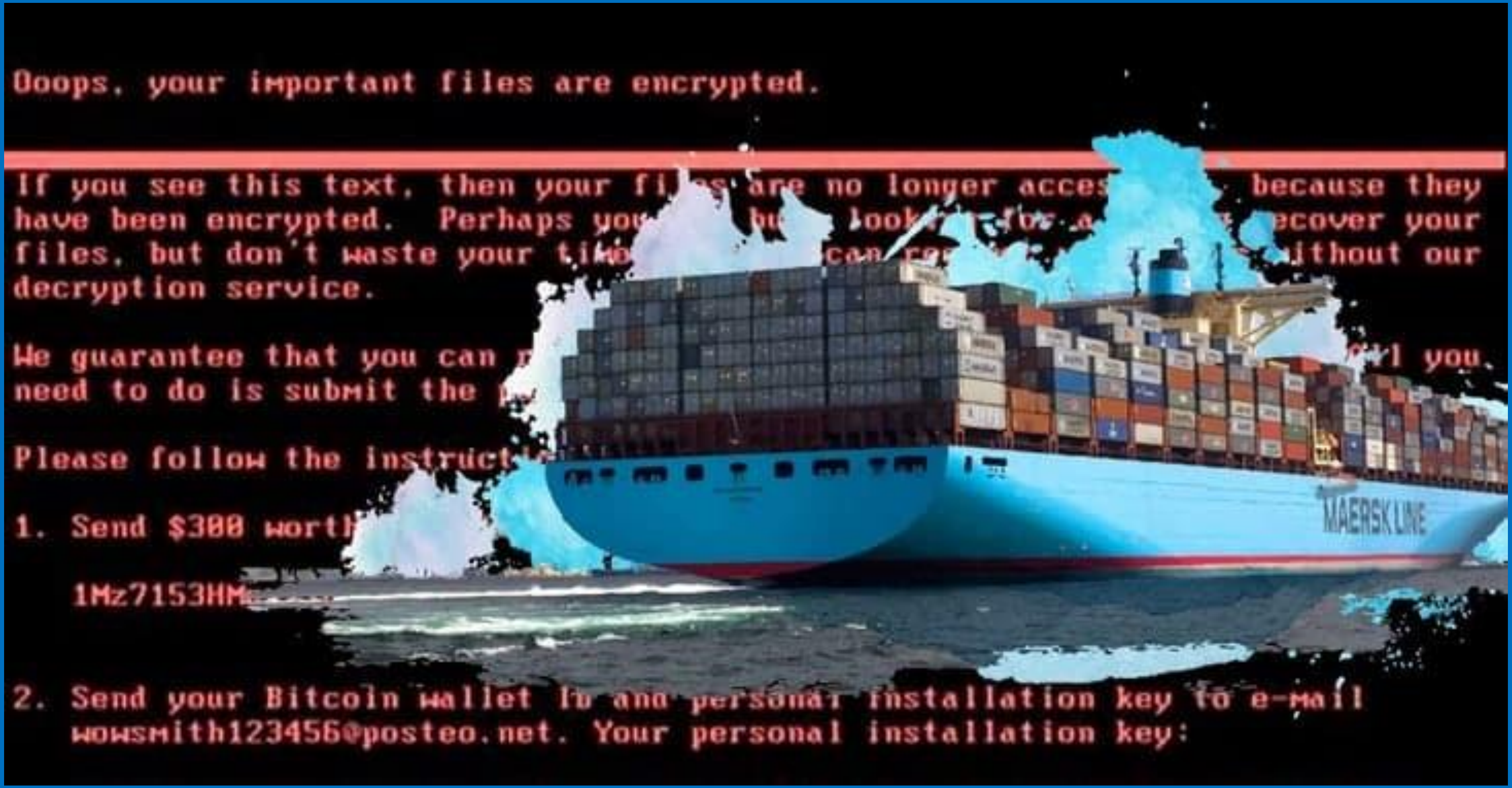
That’s what was documented in news stories.

January is just the most recent full month.

What do nearly all attacks have in common?

- We don’t know what went wrong and what they did to fix it.
- Except for Equifax in 2017, 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

Supply Chain Attack – NotPetya from 2017



```
Ooops, your important files are encrypted.

If you see this text, then your fi  s are no longer acces           because they
have been encrypted.  Perhaps you       look                  ecover your
files, but don't waste your time       can rec              ithout our
decryption service.

We guarantee that you can r                                      l you
need to do is submit the p

Please follow the instruct

1. Send $300 worth

   1Mz7153HM

2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:
```

Image and link to a great insider Maersk story from:
https://grahamcluley.com/the-inside-story-of-the-maersk-notpetya-ransomware-attack/

What’s a Supply Chain Attack?

Spy movie – good guys planning how to save the world.

Image from https://www.deadgoodbooks.co.uk/nicholas-searle-realistic-spy-movies/

What’s a Supply Chain Attack?

But the good-guy room is bugged. Bad guys are listening.

Image from https://www.deadgoodbooks.co.uk/nicholas-searle-realistic-spy-movies/

Q: How would bad guys plant bugs in every good-guy room in the world?

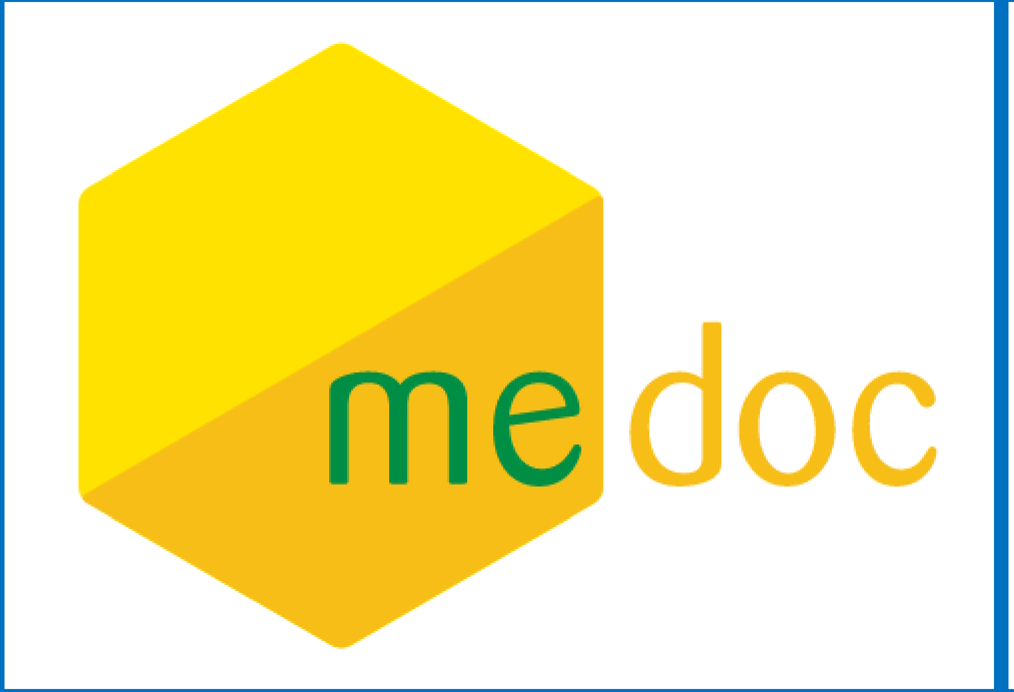
Image from https://www.deadgoodbooks.co.uk/nicholas-searle-realistic-spy-movies/

A: Take over the lightbulb factory

Plant bugs in every lightbulb.

When good guys change bulbs, bad guys own another room.

In 2017, Ukrainian Software Company, M.E. Doc was the NotPetya “Lightbulb Factory.”



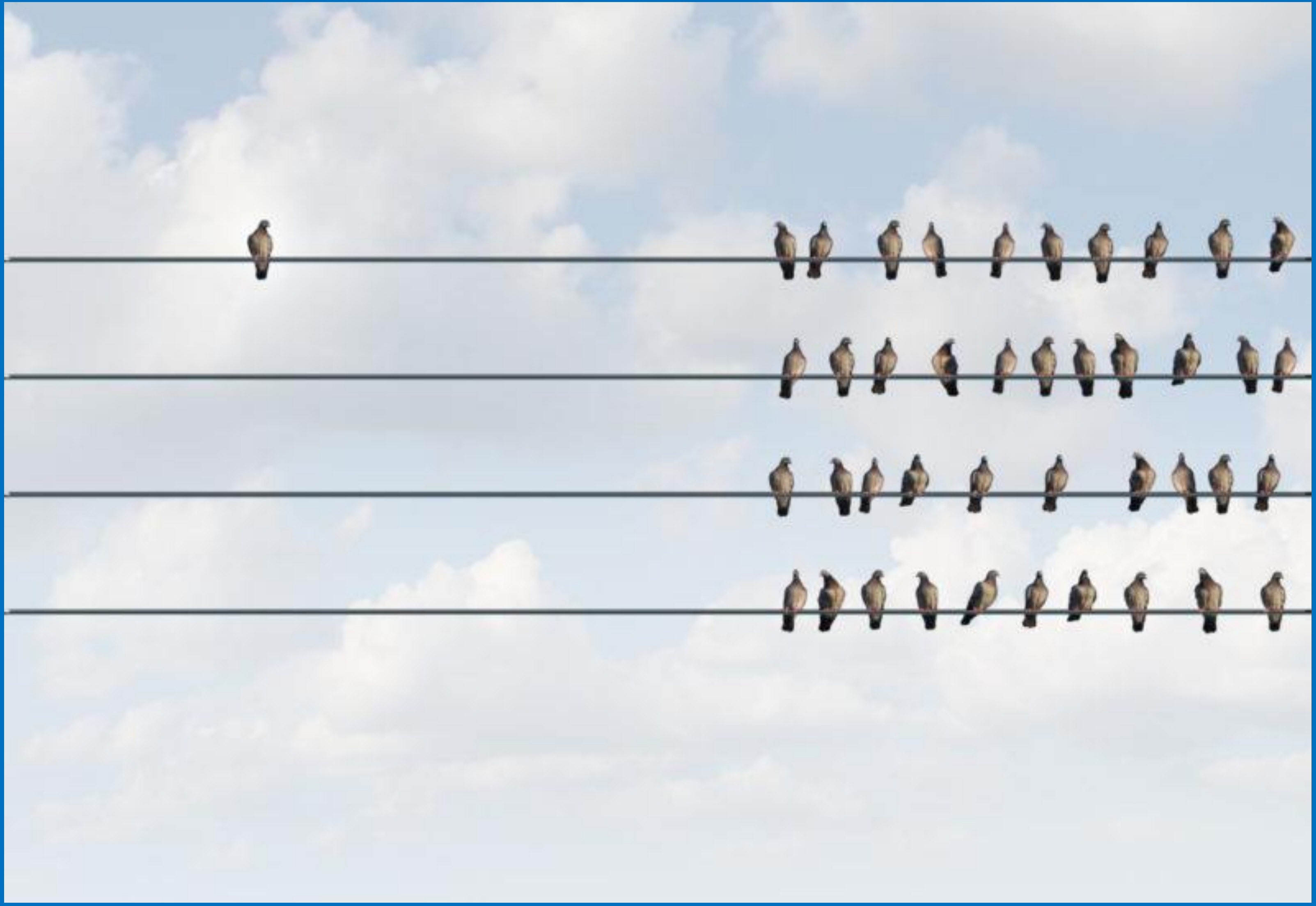
https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Supply Chain Attack: The Big One in 2020

https://www.dgregscott.com/solarwinds-fallout-so-what-and-now-what/

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?

A Solarwinds Blogger thinks so

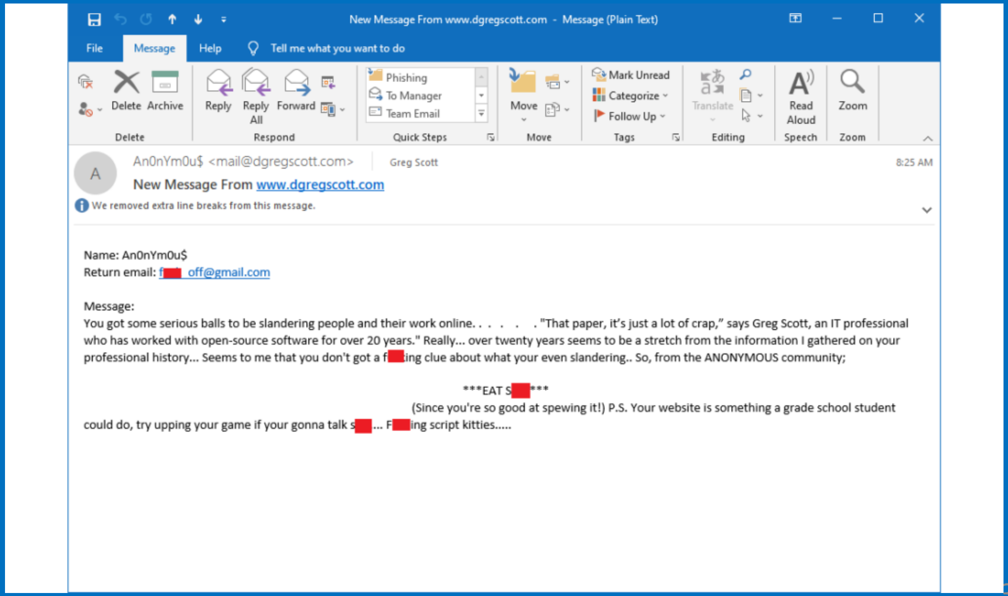
- https://thwack.solarwinds.com/resources/b/geek-speak/posts/the-pros-and-cons-of-open-source-tools
- Greg W. Stuart said…
  - [Open source] Security becomes a major issue.
    “Anyone can be hacked. However, the risk is far less when it comes to proprietary software. Due to the nature of open-source software allowing anyone to update the code, the risk of downloading malicious code is much higher.”

He posted that before Solarwinds melted down the world.

History proved him wrong.

But speaking about attempted bogus open source commits…

- See https://www.theverge.com/platform/amp/2021/4/30/22410164/linux-kernel-university-of-minnesota-banned-open-source
- Also see my blog post at https://www.dgregscott.com/nasty-letter-from-an-anonymous-knucklehead/
- Bottom line – the system worked.



AnOnYm0u$ <mail@dgregscott.com> Greg Scott 8:25 AM

New Message From www.dgregscott.com

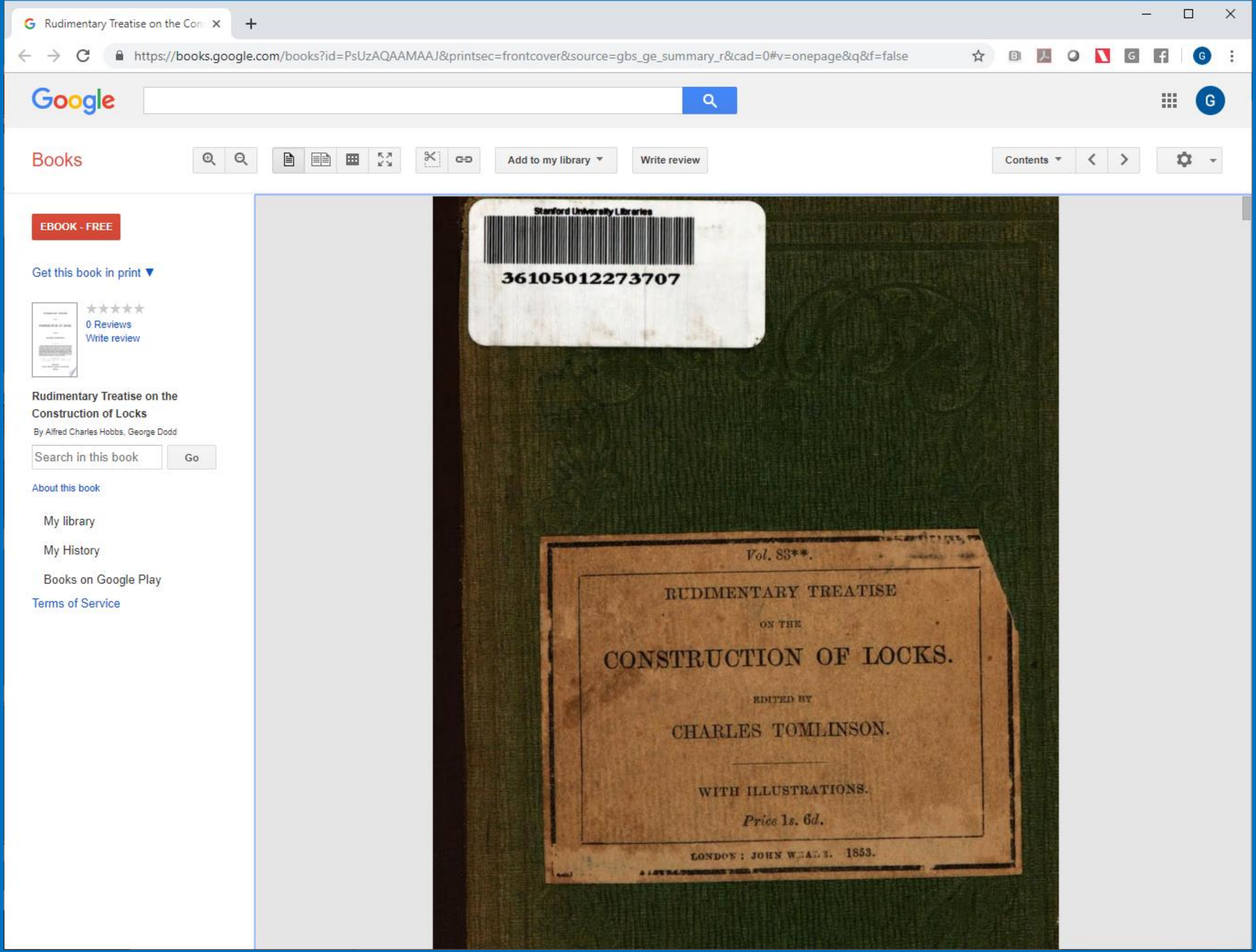
We removed extra line breaks from this message.

Name: AnOnYm0u$
Return email: f[redacted] off@gmail.com

Message:
You got some serious balls to be slandering people and their work online. . . . . . "That paper, it's just a lot of crap," says Greg Scott, an IT professional who has worked with open-source software for over 20 years." Really... over twenty years seems to be a stretch from the information I gathered on your professional history... Seems to me that you don't got a f[redacted]ing clue about what your even slandering.. So, from the ANONYMOUS community;

EAT S[redacted]

(Since you're so good at spewing it!) P.S. Your website is something a grade school student could do, try upping your game if your gonna talk s[redacted]... F[redacted]ing script kitties.....



Rudimentary Treatise on the Construction of Locks
By Alfred Charles Hobbs, George Dodd

Stanford University Libraries
36105012273707

Vol. 83**.

RUDIMENTARY TREATISE
ON THE
CONSTRUCTION OF LOCKS.
EDITED BY
CHARLES TOMLINSON.
WITH ILLUSTRATIONS.
Price 1s. 6d.
LONDON: JOHN WEALE. 1853.

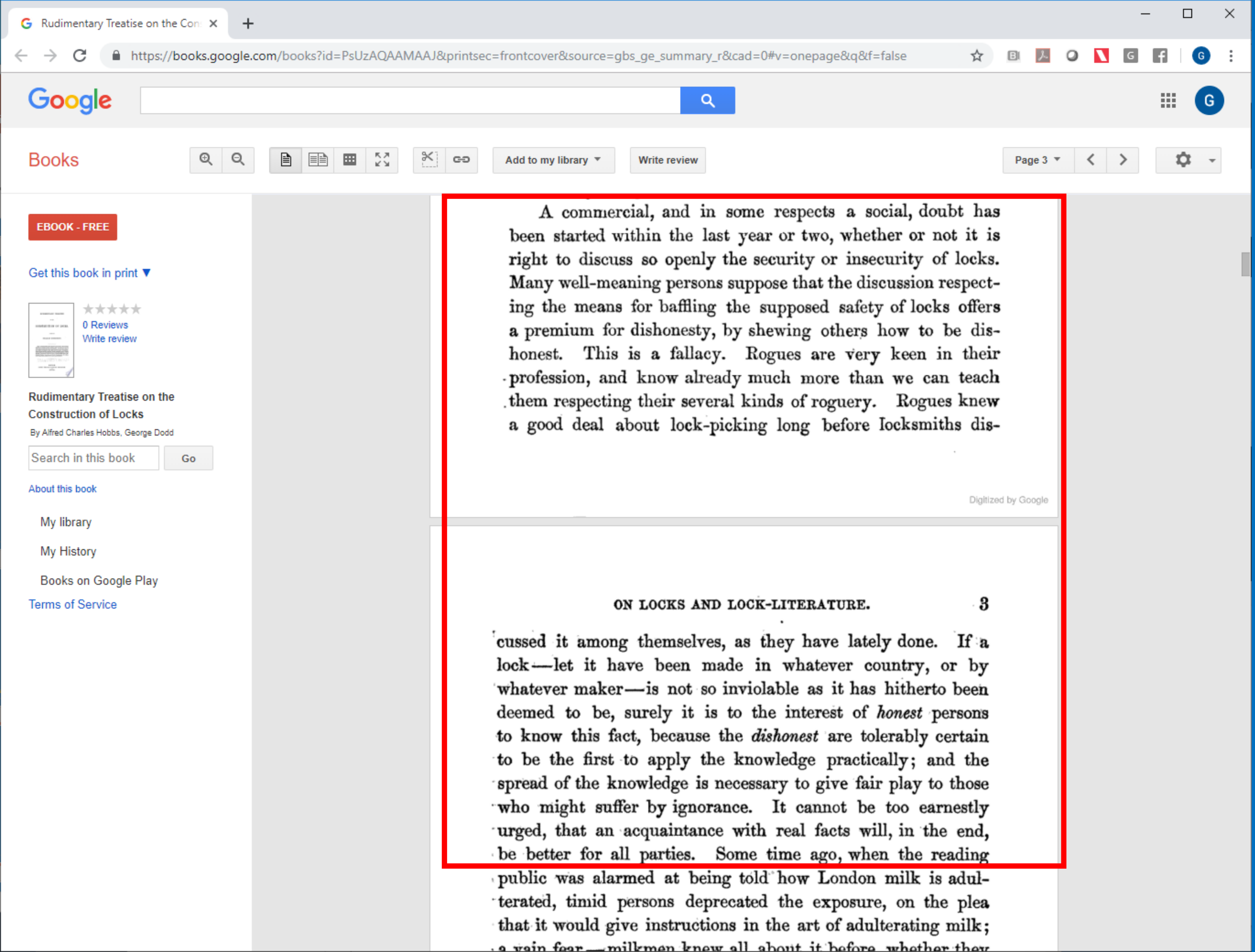
Controversy around embracing open goes back to at least 1853

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

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-

Digitized by Google

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.

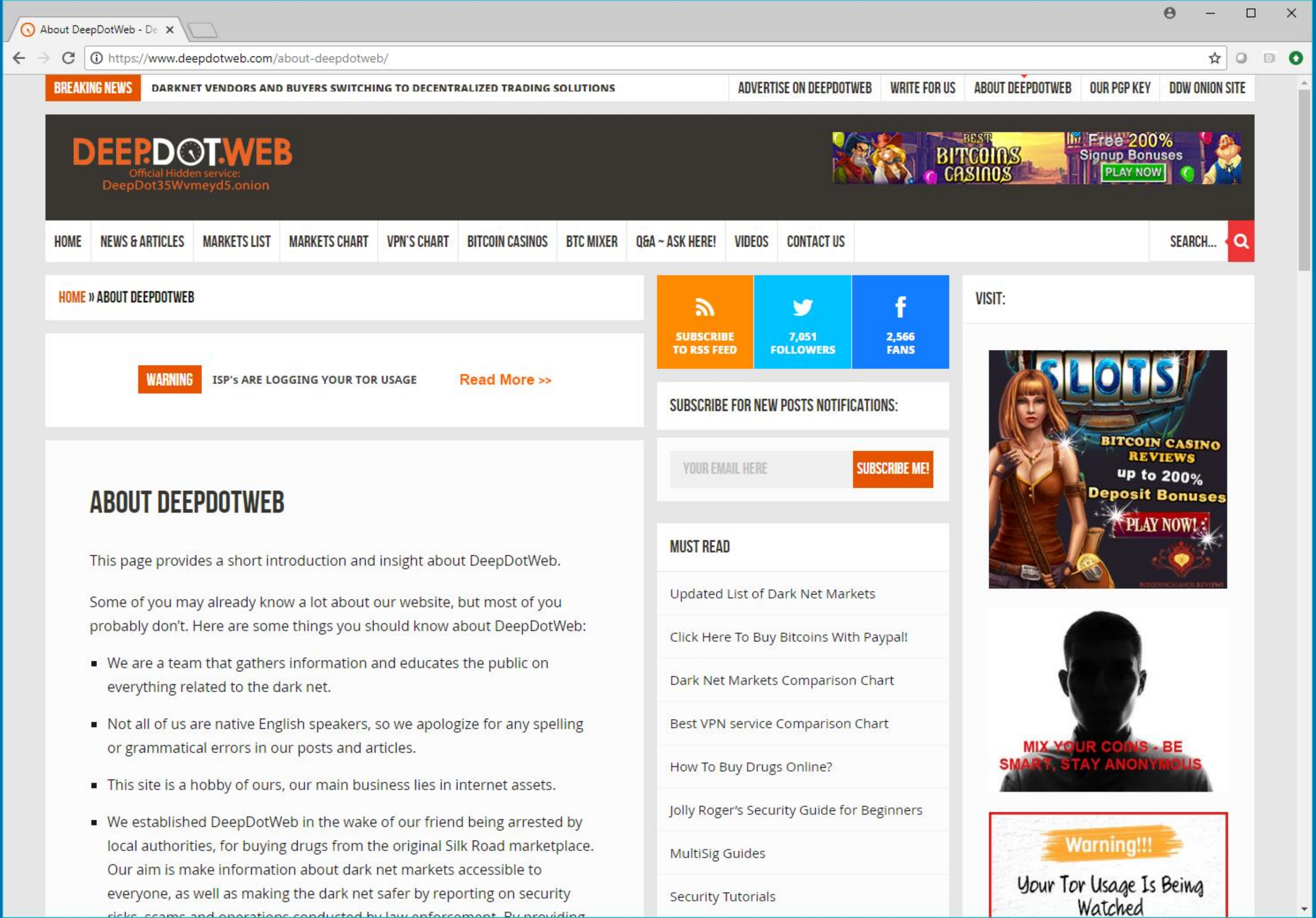
Rogues are Very keen in their profession, and know already much more than we can teach them respecting their several kinds of roguery. Rogues knew a good deal about lock-picking long before locksmiths discussed it among themselves, as they have lately done.

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.

21st century 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.
  - That's why we keep making the same mistakes.
- We need to level the playing field.



ABOUT DEEPDOTWEB

This page provides a short introduction and insight about DeepDotWeb.

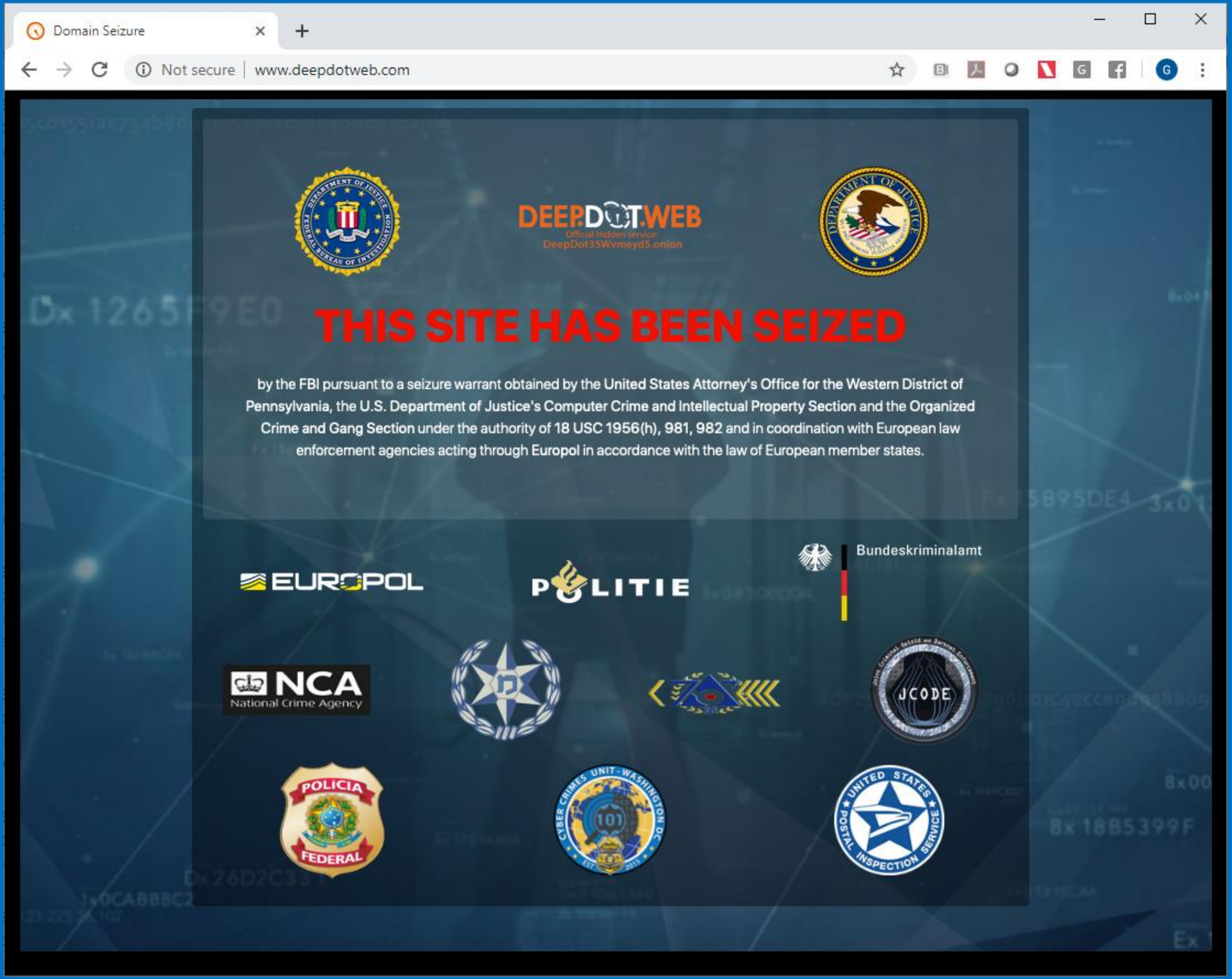
Some of you may already know a lot about our website, but most of you probably don't. Here are some things you should know about DeepDotWeb:

- 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



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.

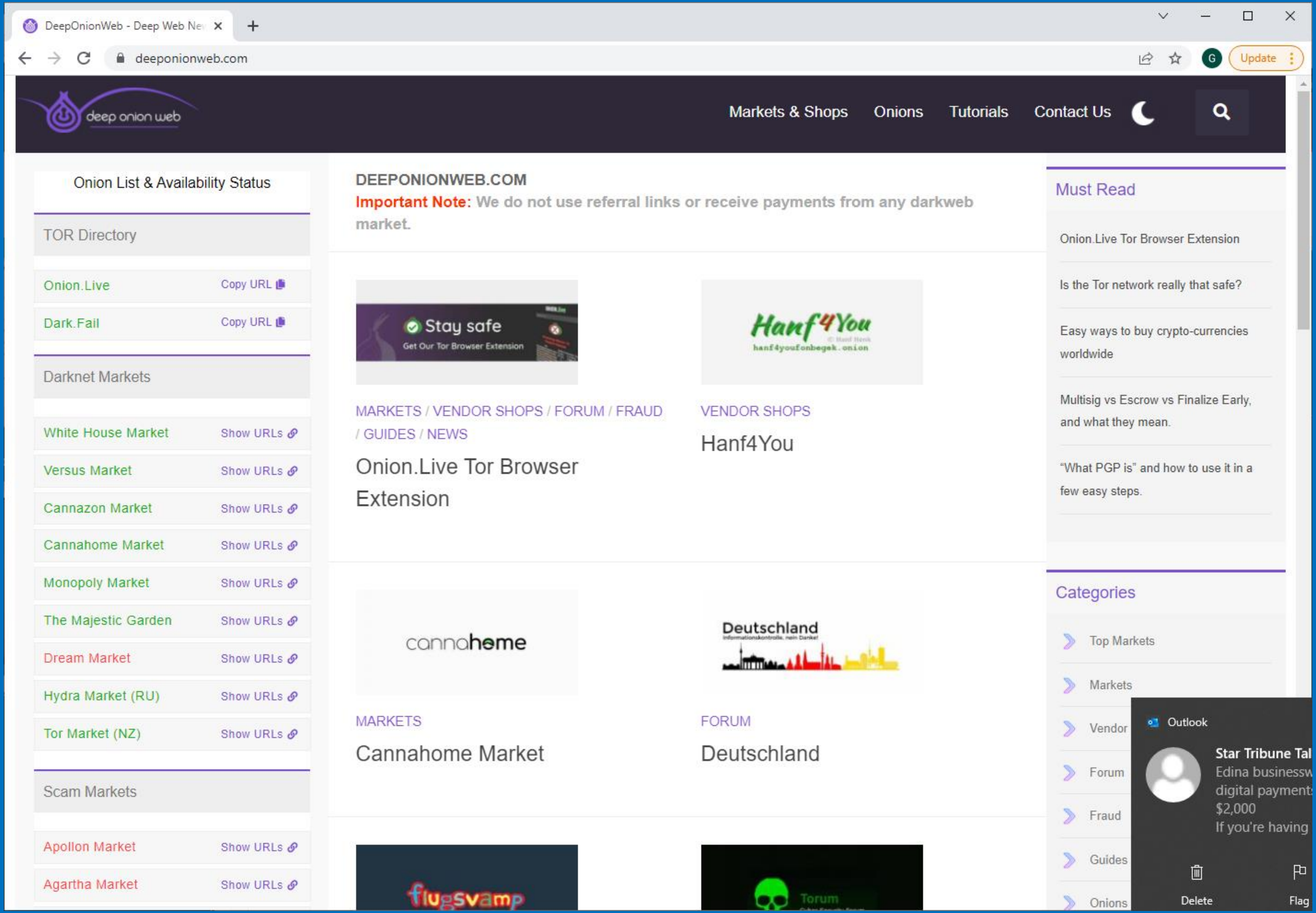
Check out this article from Wired Magazine:

https://www.wired.com/story/dark-web-drug-takedowns-deepdotweb-rebound/

Score one for the good guys.

But Bad Guys Don’t Give Up Easily

- https://www.deeponionweb.com/



Onion List & Availability Status

TOR Directory

Onion.Live	Copy URL
Dark.Fail	Copy URL

Darknet Markets

White House Market	Show URLs
Versus Market	Show URLs
Cannazon Market	Show URLs
Cannahome Market	Show URLs
Monopoly Market	Show URLs
The Majestic Garden	Show URLs
Dream Market	Show URLs
Hydra Market (RU)	Show URLs
Tor Market (NZ)	Show URLs

Scam Markets

Apollon Market	Show URLs
Agartha Market	Show URLs

DEEPONIONWEB.COM

Important Note: We do not use referral links or receive payments from any darkweb market.

MARKETS / VENDOR SHOPS / FORUM / FRAUD / GUIDES / NEWS

Onion.Live Tor Browser Extension

VENDOR SHOPS

Hanf4You

MARKETS

Cannahome Market

FORUM

Deutschland

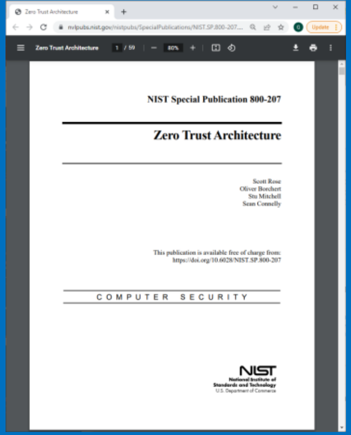
Must Read

- Onion.Live Tor Browser Extension
- Is the Tor network really that safe?
- Easy ways to buy crypto-currencies worldwide
- Multisig vs Escrow vs Finalize Early, and what they mean.
- “What PGP is” and how to use it in a few easy steps.

Categories

- Top Markets
- Markets
- Vendor
- Forum
- Fraud
- Guides
- Onions

Zero Trust Architecture


Zero Trust Architecture
nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207....
Update
Zero Trust Architecture
1 / 59
80%

NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

COMPUTER SECURITY

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

- NIST (United States National Institute of Standards) framework called *Special Publication 800-207*.
    1. The entire enterprise private network is not considered an implicit trust zone.
    2. Devices on the network may not be owned or configurable by the enterprise.
    3. No resource is inherently trusted.
    4. Not all enterprise resources are on enterprise-owned infrastructure.
    5. Remote enterprise subjects and assets cannot fully trust their local network connection.
    6. Assets and workflows moving between enterprise and non-enterprise infrastructure should have a consistent security policy and posture.

- Helpful because it makes realistic assumptions about how modern networks should operate.
- But the real world rarely follows theoretical architectures.

There will ***never*** be a technology defense against supply chain attacks.

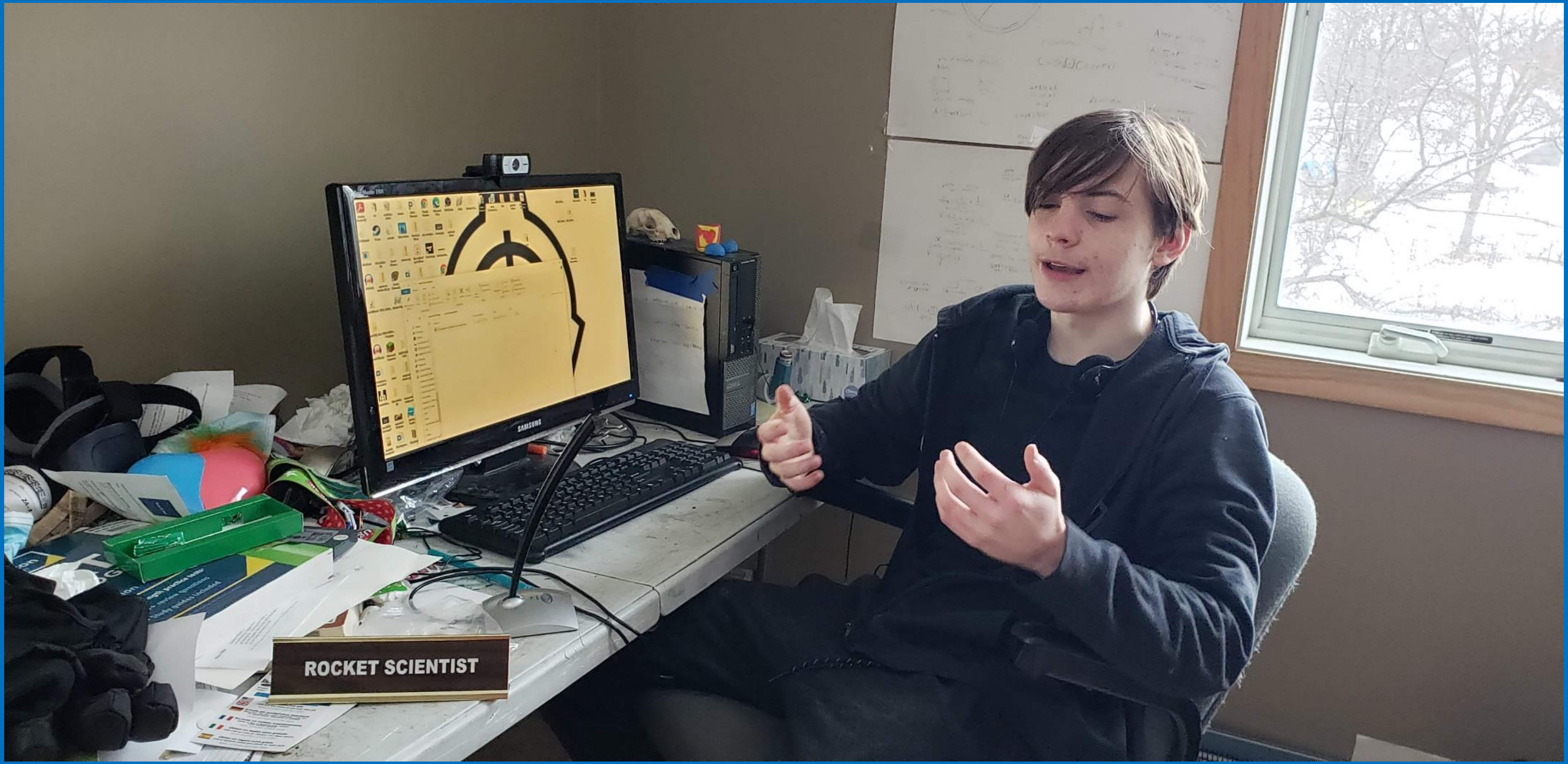
Because you ***always*** need to trust somebody.

The only defense:

- Make suppliers earn your trust.
- Suppliers earn trust by embracing open.

Call to Action

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

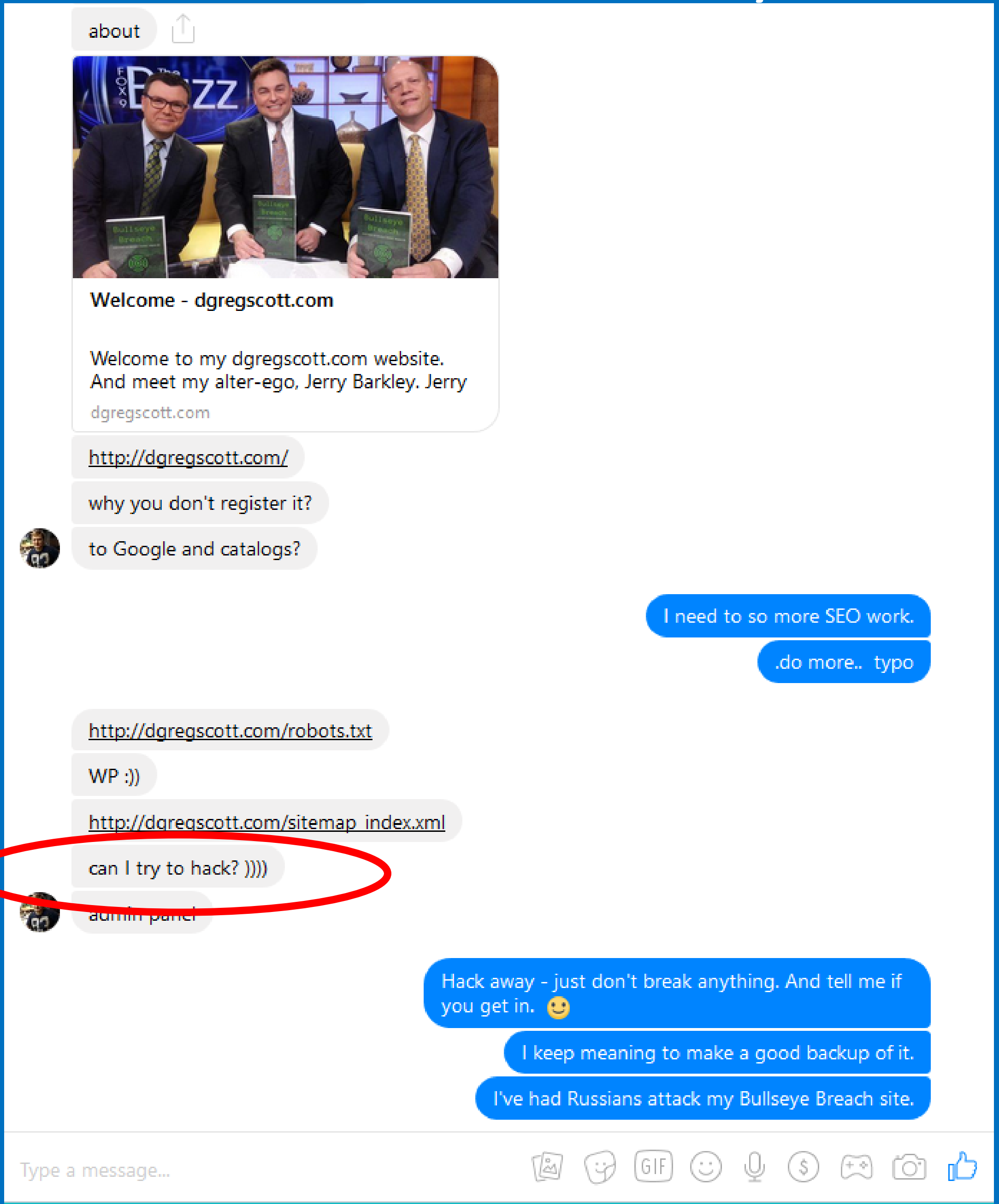
From https://www.businessinsider.com/warren-buffett-cybersecurity-berkshire-hathaway-meeting-2017-5

Or Delta CISO Debbie Wheeler

- “We have to get to the point where security can’t be seen as a competitive advantage; it can’t be what we use to succeed against a competitor. Security has to be one of those areas where we come together to share best practices. Some of those might not be for everyone, but the sharing of them will serve us all and help us all to be stronger. And that’s what we need.”
- https://www.csoonline.com/article/3649355/delta-ciso-debbie-wheeler-security-can-t-be-seen-as-a-competitive-advantage.html

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

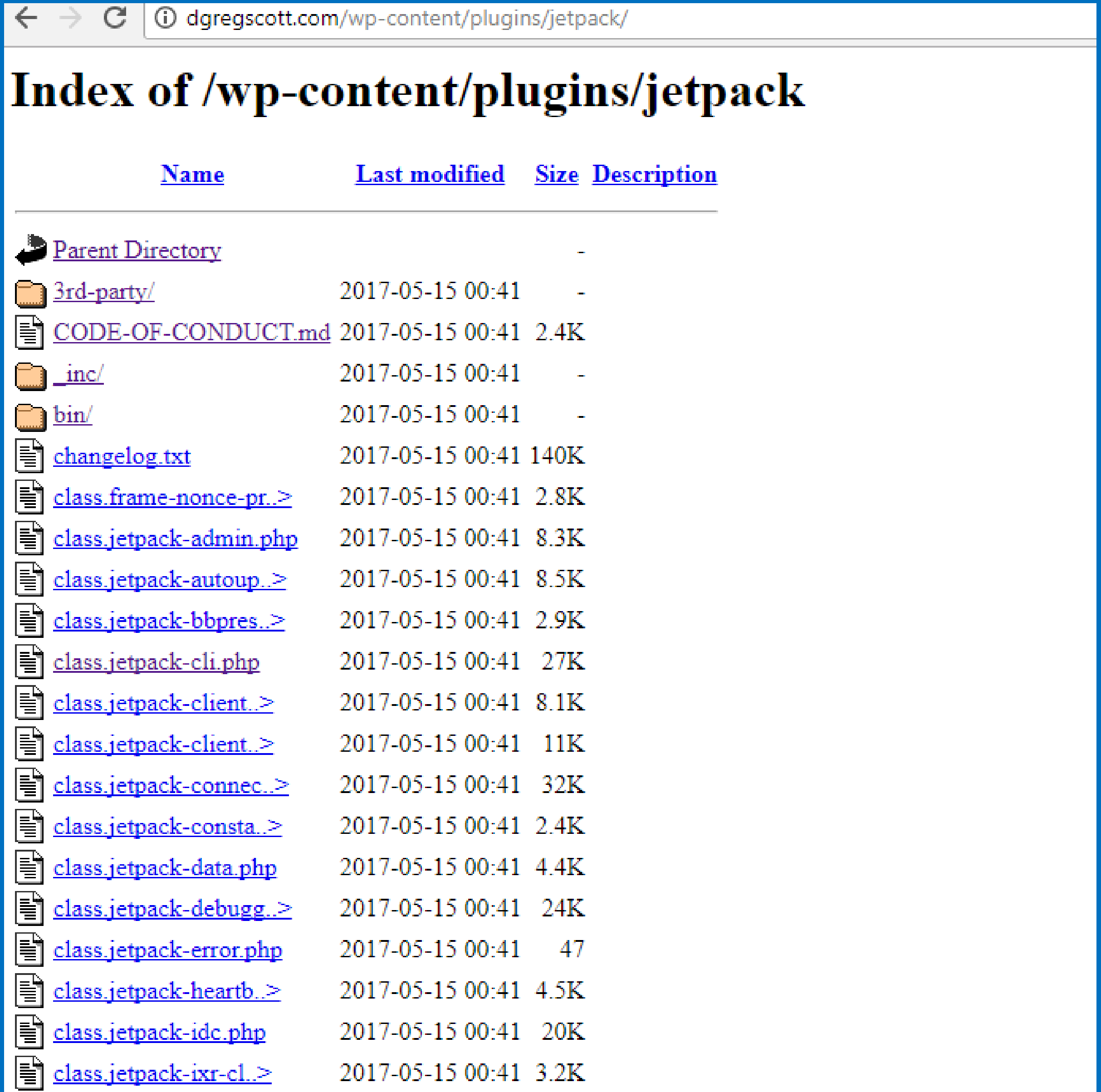
Hack away - just don't break anything. And tell me if you get in. 🙂

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))



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	

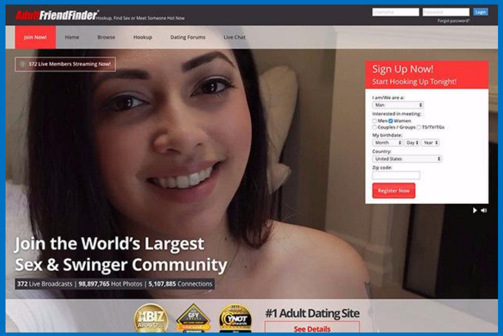
The cure

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>
```



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

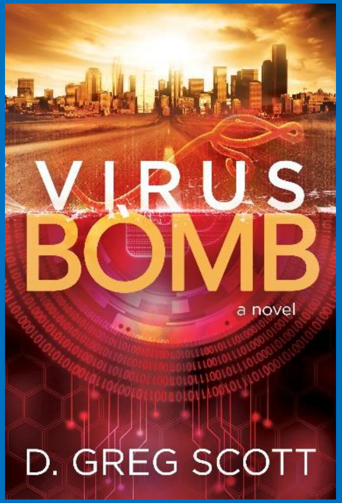
What if organizations like these embraced open?

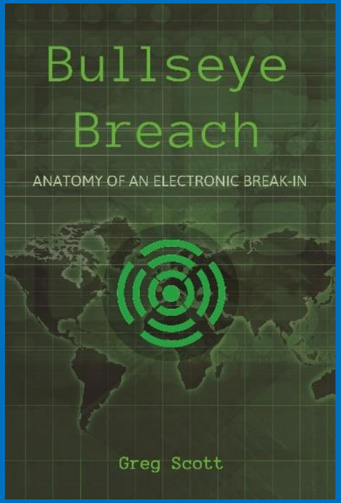
- Equifax may have saved more than $1 billion in remediation costs.
- Uber would not have become an unwitting partner with people who stole from it.
- Ransomware attacks might not have disrupted Atlanta, Baltimore, and dozens of other cities recently.
- Solarwinds might not have compromised pretty much all the world’s critical infrastructure.
- Fuel deliveries across the Eastern United States would never have been disrupted.
- (Your organization here)

Contact info

—D. Greg Scott—

gregscott@infrasupport.com or
gregscott@dgregscott.com





https://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