CSE508 Network Security

Stony Brook University

2021-05-06

Anonymity

Michalis Polychronakis

Stony Brook University

Privacy

“The right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share information about itself with others.” [RFC2828]

Anonymity

“The state of being not identifiable within a set of subjects, the anonymity set.” [Pfitzmann and Köhntopp]

Very different from privacy:

> An anonymous action may be public, but the actor’s identity remains unknown (e.g., vote in free elections)

Operations Security (**OPSEC**)

Main goal: c*ontrol information about capabilities and intentions to prevent their exploitation by the adversary*

- Term coined by the US military during the Vietnam War

OPSEC process

- Identify critical information
- Determine if friendly actions can be observed by enemy intelligence
- Determine if information obtained by adversaries could be interpreted to be useful to them
- Execute selected measures that eliminate or reduce adversary exploitation of friendly critical information

OPSEC in Cybersecurity

Protect the real identity of someone who has chosen to operate under a pseudonym

- Blackhat or whitehat

Prevent adversaries from obtaining data that can be used to disclose sensitive personal information

- Doxxing, extortion, shaming, …

Prevent the collection of information that can aid in breaching security

- Reconnaissance, social engineering, …

Broader scope: protect user privacy

- PII leakage, online tracking, behavioral profiling, …

Critical OPSEC Risk: Contamination

Even the slightest connection or contact between the real identity and an alias can lead to contamination

- In both the online and offline world
- IP addresses, device identifiers, configurations, language, writing style, email accounts, usernames, personal traits, timing patterns, location, …

Cover identities should be kept completely isolated

- Any contact between personas contaminates both

Must be very careful…

- Maintaining good OPSEC for long periods of time is *stressful*
- Increased OPSEC comes at the cost of *efficiency*

http://grugq.github.io/presentations/Keynote_The_Grugq_-_OPSEC_for_Russians.pdf

Don’t include personal information in your username

Don’t discuss personal traits such as gender, profession, hobbies, beliefs, …

Don’t use special characters unique to your language

Don’t keep regular hours/habits (can reveal timezone/geographic location)

Don’t talk about the environment (weather, politics, culture, …)

Don’t talk about your other identities

Don’t use social media

Don’t use the same device for different identities

Don’t use different devices from the same location

…

http://grugq.github.io/presentations/Keynote_The_Grugq_-_OPSEC_for_Russians.pdf

Anonymous Communication

Sender anonymity

The identity of the party who sent a message is hidden, while its receiver (and the message itself) might not be

Receiver anonymity

The identity of the receiver is hidden

Unlinkability of sender and receiver

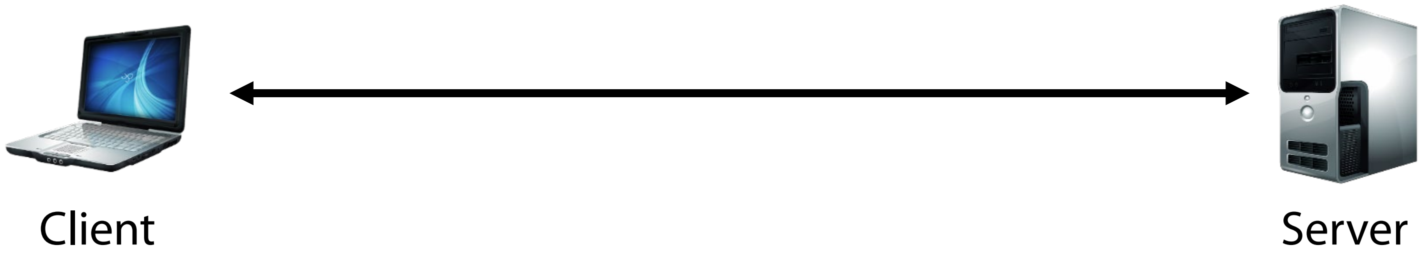
Although the sender and receiver can each be identified as participating in some communication, they cannot be identified as communicating with each other

The internet was not designed for anonymity

Packets have source and destination IP addresses

Using pseudonyms to post anonymously is not enough…

The server always sees the IP address of the client



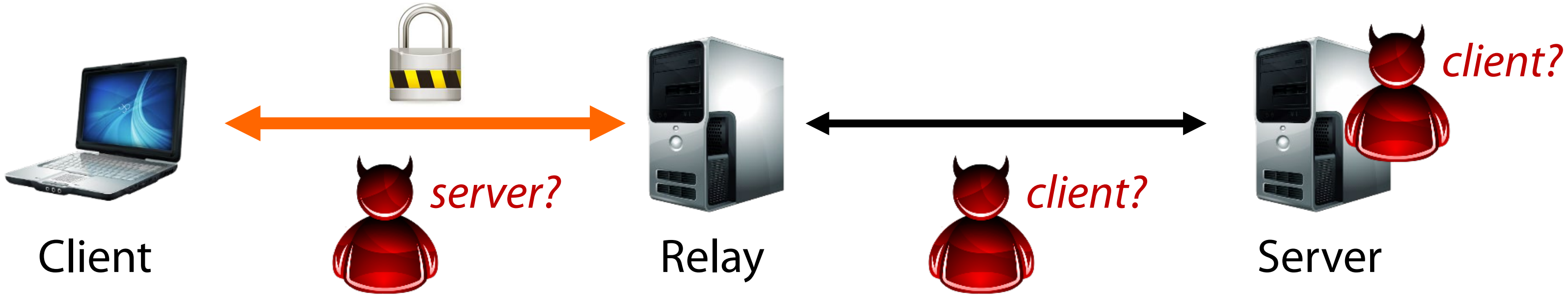
Need to hide the source IP address

(Assuming no other PII is revealed – *OPSEC is hard)*

Stepping Stones: (Fake Sense of) Anonymity

Proxies, relays, VPN servers

- Destination server sees only the relay's IP address *(but the relay knows the client's IP)*
- Since the relay cooperates, let's also encrypt the connection to it



Sender anonymity against the server and observers beyond the relay

Also: receiver anonymity against local network observers

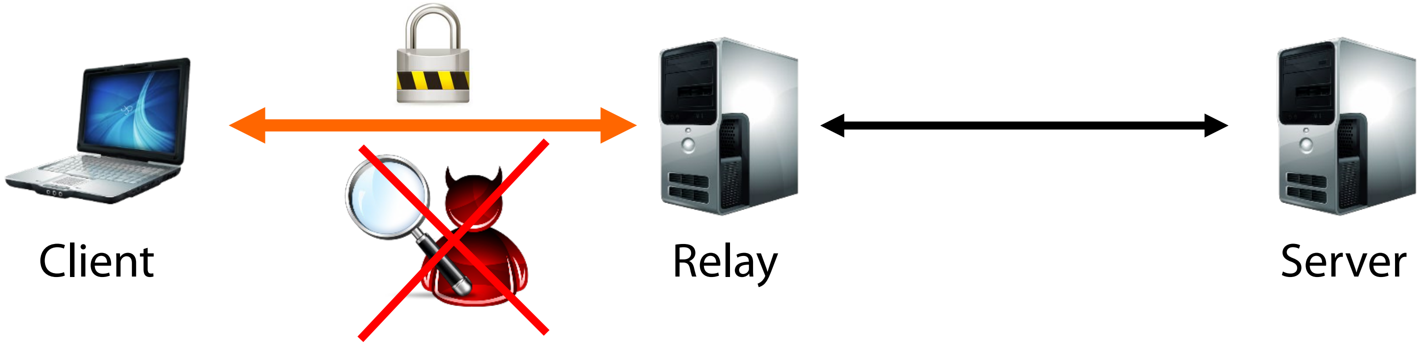
- All they see is client ⇔ relay connections (the encrypted tunnel hides the destination)

Stepping Stones: Traffic Protection

The encrypted client ⇔ relay channel protects against *local adversaries*

The definition of "local" depends on the location of the relay

Users in the same LAN, employer's admins, ISPs, governments, …



Protection against passive/active adversaries (sniffing, MitM, MotS, …)

In addition to the use of end-to-end encryption (e.g., TLS)

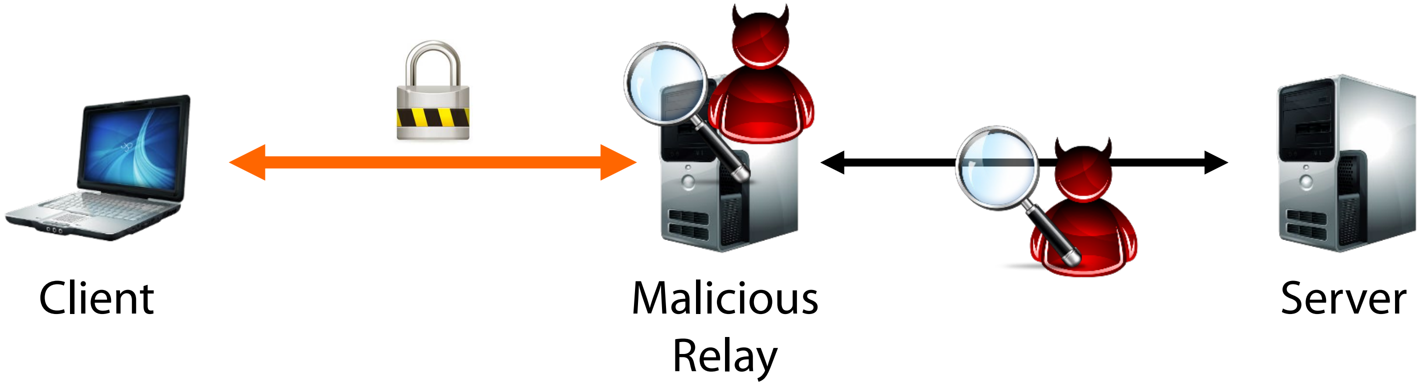
Policy and censorship circumvention

Parental controls, company-wide port/domain/content blocking, country-specific media content, hotel WiFi restrictions, government censorship, …

Stepping Stones: What about other adversaries?

The relay itself may be the adversary – can see it all!

Network observers beyond the relay can see it all!



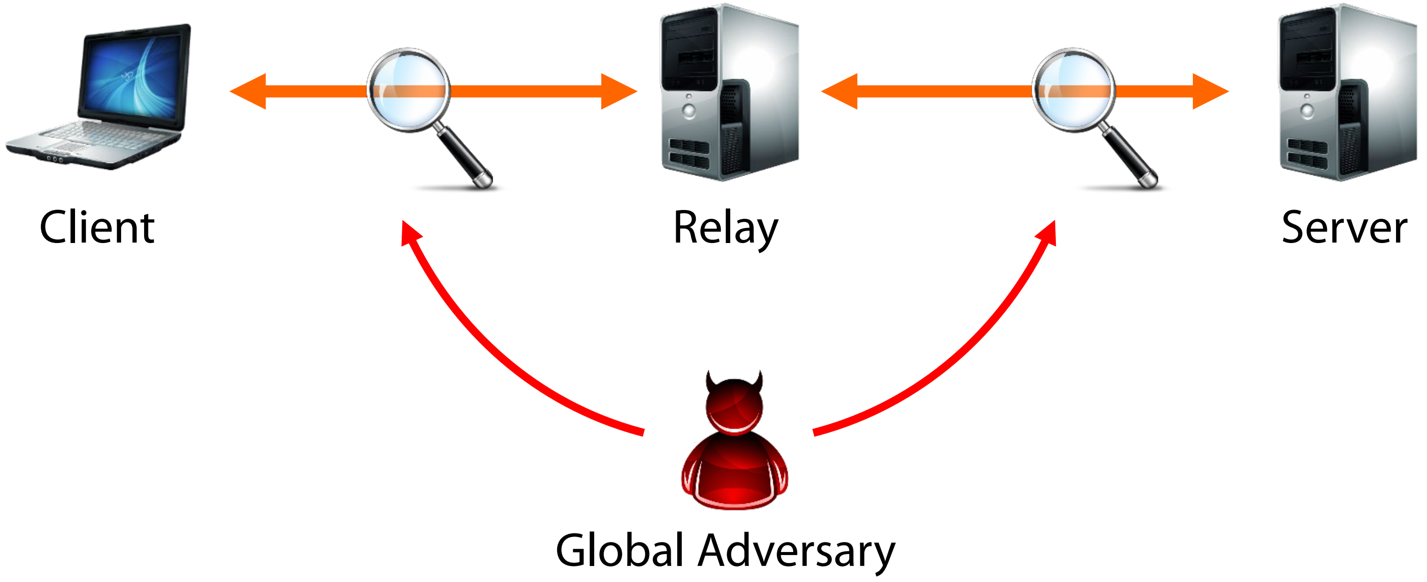
Adversaries who couldn't eavesdrop before, now can: just set up a rogue proxy or VPN server and lure users

End-to-end encryption is critical!

Stepping Stones: Global Adversaries

A "global" adversary may be able to observe both ends

Traffic analysis: communication patterns can be observed even when end-to-end encryption is used



Eavesdropping vs. Traffic Analysis

Even when communication is encrypted, the mere fact that two parties communicate reveals a lot

Example: what can we learn from phone records?

- Who communicated with whom and when
- Activity patterns (periodic, time of day, occasional, …)
- Single purpose numbers (hotlines, agencies, doctors, …)

It’s not “just metadata”…

Network traffic analysis can reveal a lot

Passive traffic analysis

Frequency and timing of packets, packet sizes, amount of transferred data, …

Active traffic analysis

Packet injection, fingerprint injection by manipulating traffic characteristics, …

Examples:

Message timing correlation to learn who is talking to whom

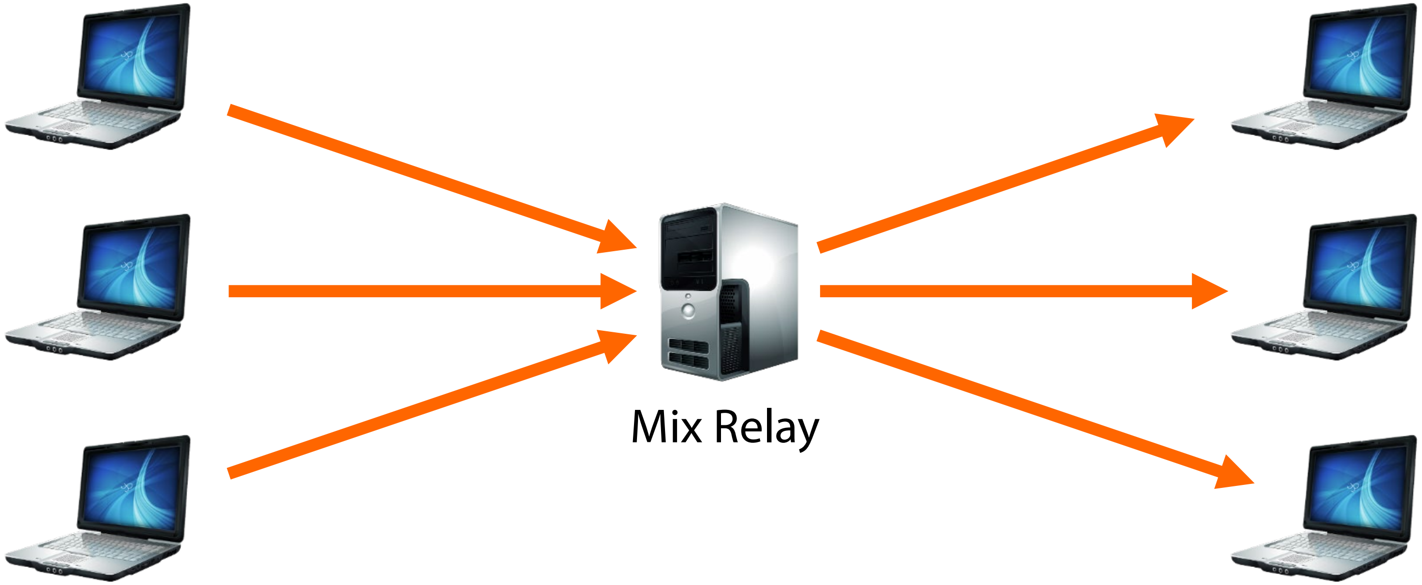
Fingerprinting of visited HTTPS web pages through structural analysis (DNS requests, number/size of embedded elements, etc.)

SSH keystroke timing analysis

> *"Traffic analysis, not cryptanalysis, is the backbone of communications intelligence."*
>
> — Susan Landau and Whitfield Diffie

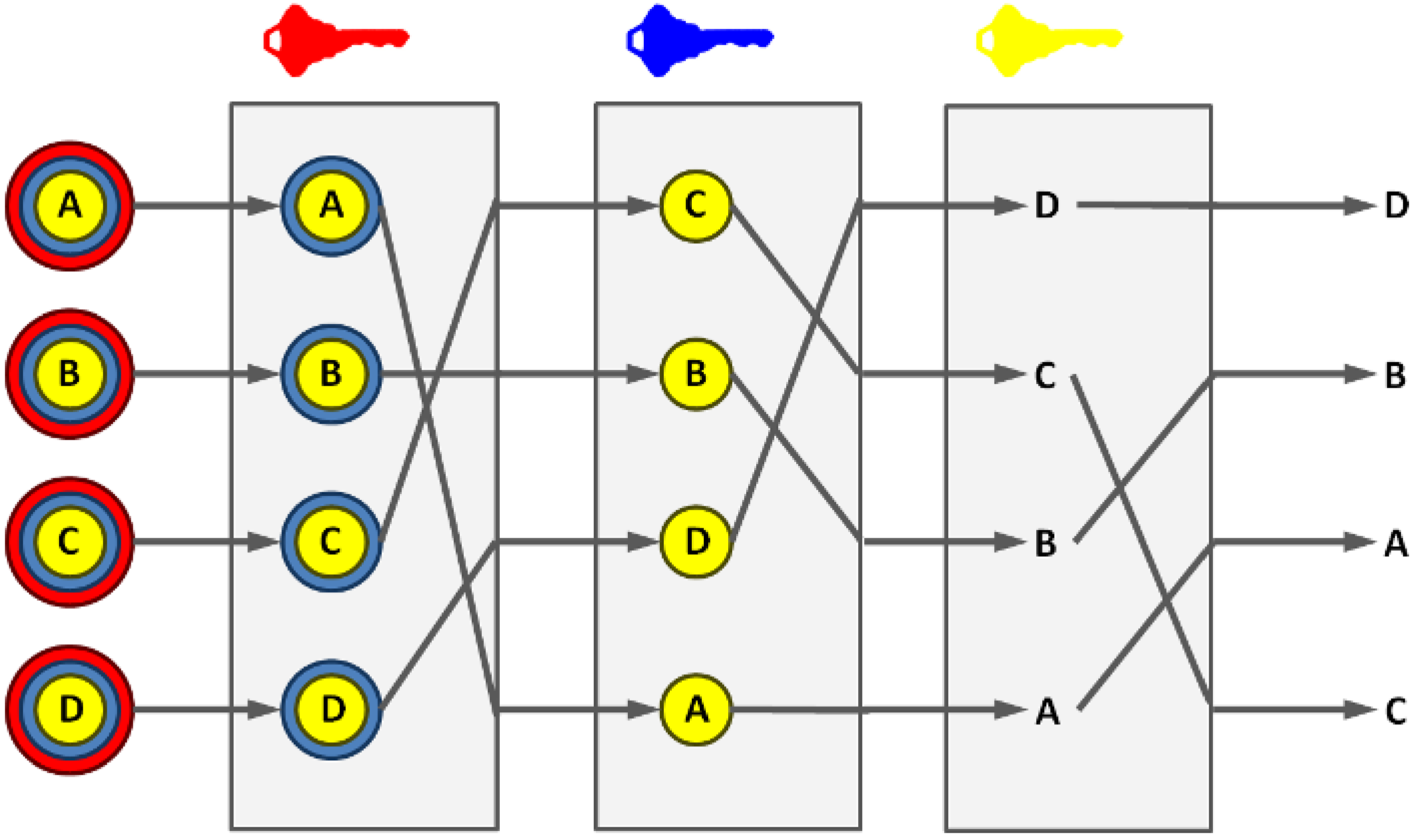
Mix Networks [Chaum 1981]

Main idea: hide own traffic among others' traffic



Originally conceived for anonymous email: Trusted remailer + public key crypto

Additional measures are critical for thwarting traffic analysis: message padding, delayed dispatch, dummy traffic



Adding multiple mix relays allows for anonymity even if some relays are controlled by an adversary

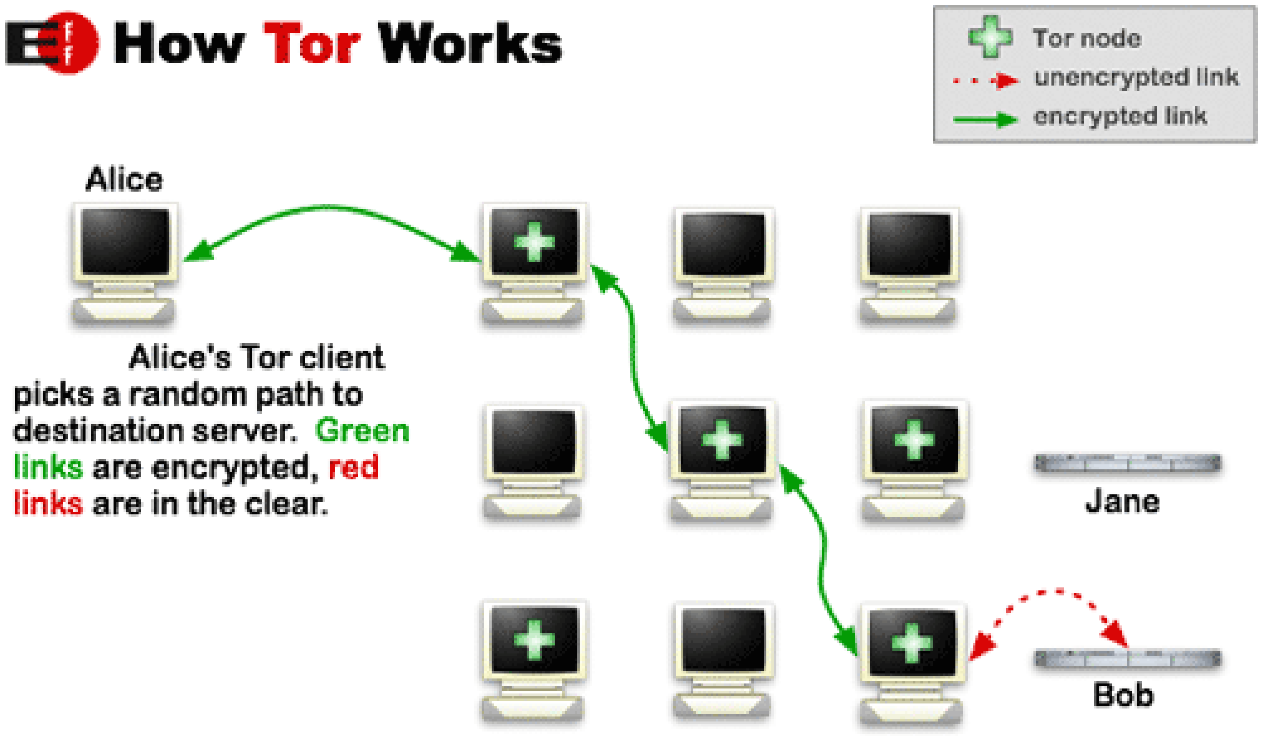
- Deanonymization still possible if the adversary controls *all* relays of a circuit
- Main drawback: prohibitively high latency for interactive communication

https://en.wikipedia.org/wiki/Mix_network

Tor (aka. the Onion Router)

Low-latency anonymous communication network

Layered encryption: each relay decrypts a layer to reveal only the next relay


How Tor Works
Tor node
unencrypted link
encrypted link
Alice
Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
Jane
Bob

© Tor Project - https://www.torproject.org/about/overview.html.en

Tor (aka. the Onion Router)

Worldwide volunteer network of ~7K relays

- ~2.5M daily users
- ~600 Gbit/s advertised bandwidth, ~300 Gbit/s consumed

Three-hop circuits by default

- Entry node, middle node, exit node
- Longer circuits can be built
- Multiple connections can be multiplexed over the same Tor circuit

Directory servers point to active Tor relays

- 10 directory servers hard-coded into the Tor client
- Monitoring for mass subscriptions by potential adversaries (sybil attack)

https://metrics.torproject.org/

Applications

User-friendly Tor Browser

- Additional measures to thwart web tracking and fingerprinting

TAILS Linux distribution (The Amnesic Incognito Live System)

- Forces *all* outgoing connections to go through Tor - **USE THIS!!!**

Onion services: hide the IP address of *servers*

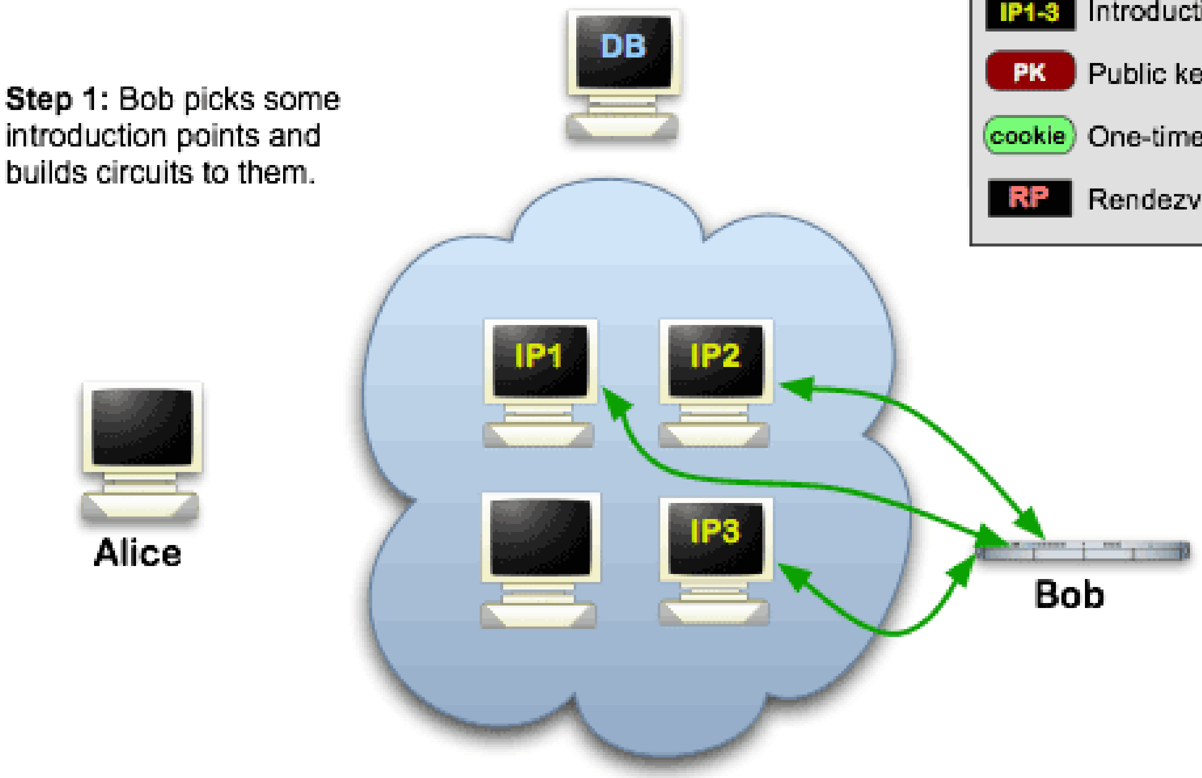
- `.onion` pseudo top-level domain host suffix
- Not always easy: misconfigurations and leaks may reveal the server's real IP address

SecureDrop (originally designed by Aaron Swartz)

- Platform for secure anonymous material submission and communication between sources (whistleblowers) and journalists

Many more: OnionShare (file sharing), Ricochet (IM), …

Onion Services: Step 1

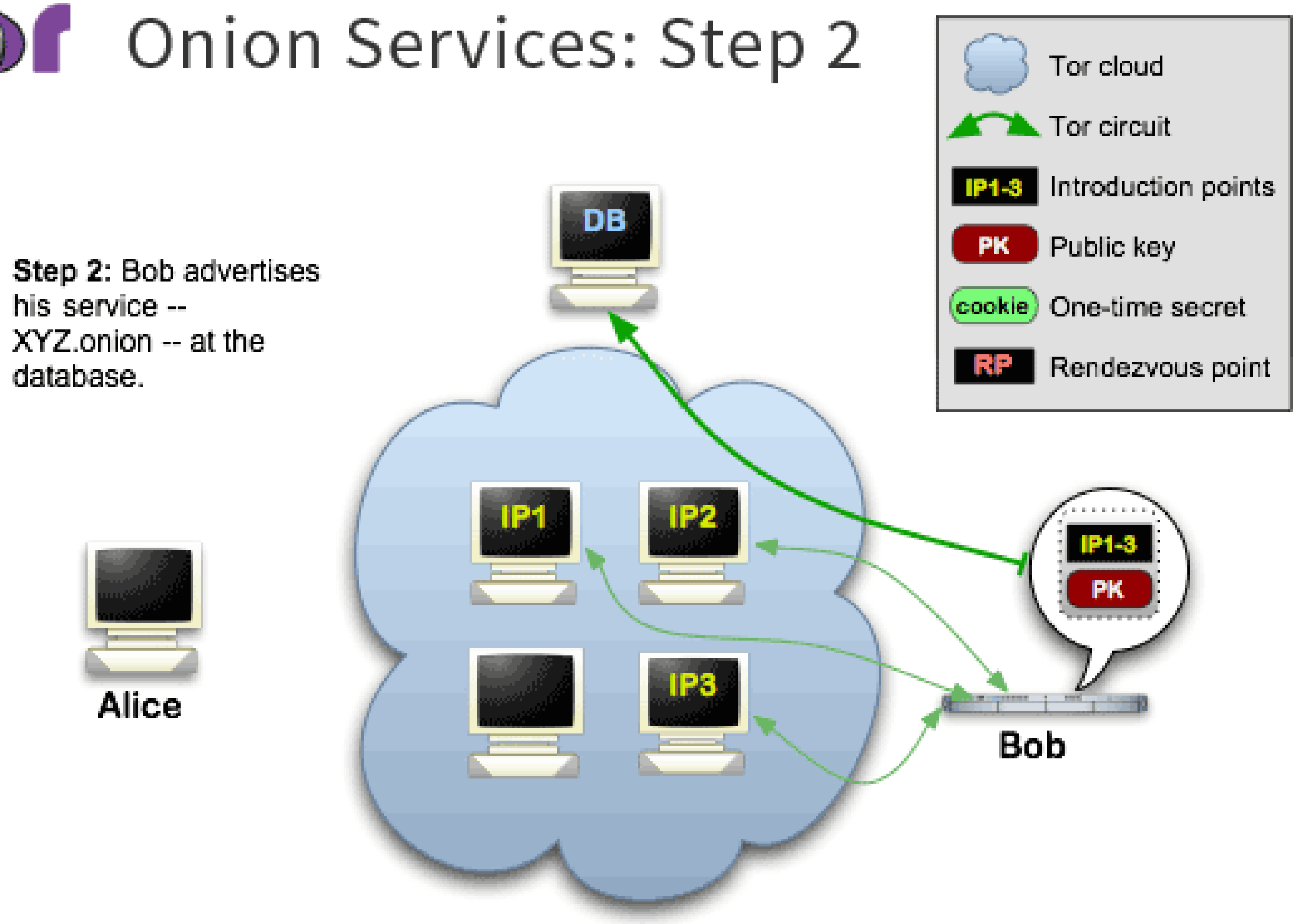


Step 1: Bob picks some introduction points and builds circuits to them.

☁	Tor cloud
⟷	Tor circuit
IP1-3	Introduction points
PK	Public key
cookie	One-time secret
RP	Rendezvous point

https://www.torproject.org/docs/onion-services.html.en

Onion Services: Step 2

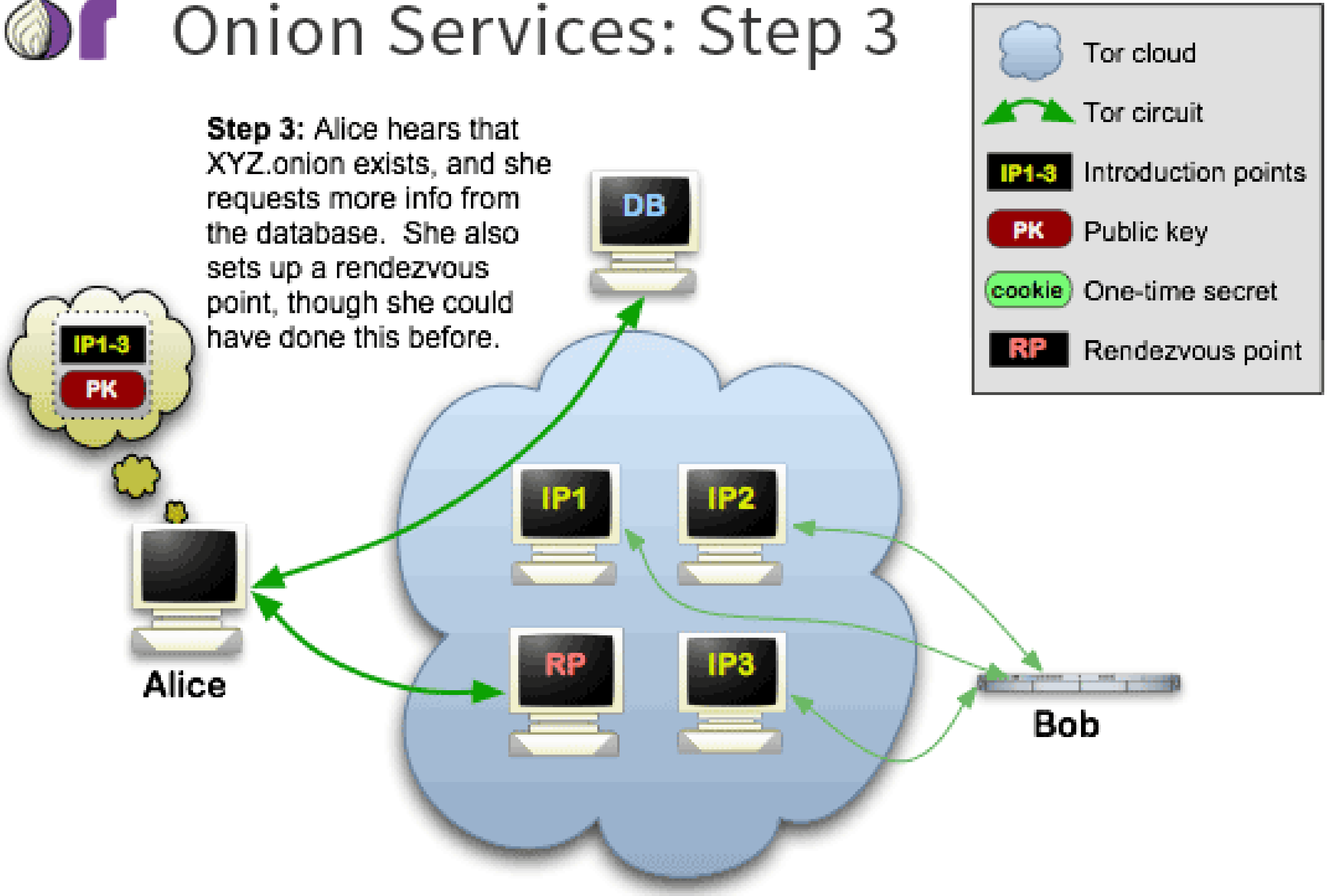


Step 2: Bob advertises his service -- XYZ.onion -- at the database.

Onion addresses are self-authenticating: derived from the service's public key (e.g., http://expyuzz4wqqyqhjn.onion/)

https://www.torproject.org/docs/onion-services.html.en

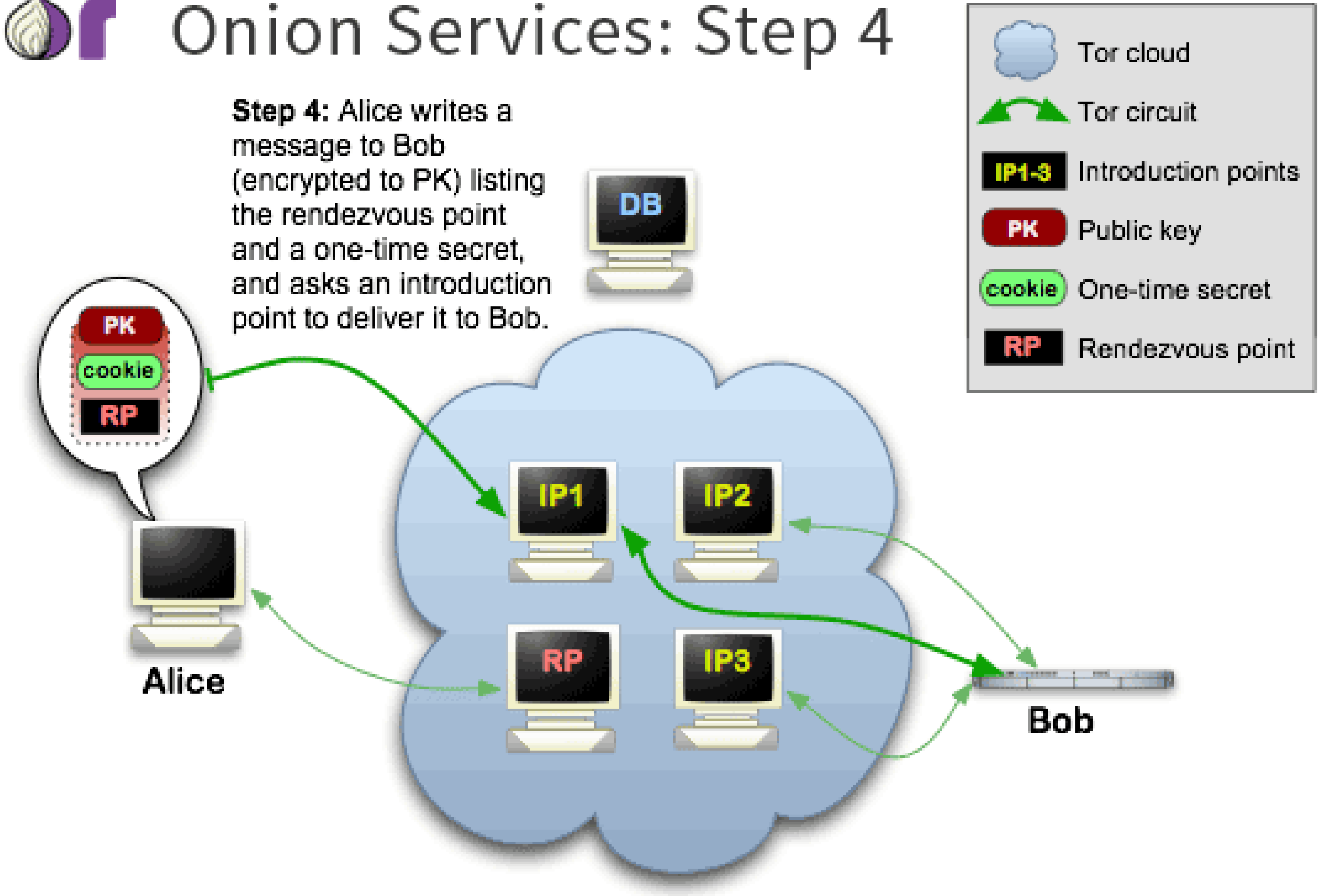
Onion Services: Step 3



Step 3: Alice hears that XYZ.onion exists, and she requests more info from the database. She also sets up a rendezvous point, though she could have done this before.

https://www.torproject.org/docs/onion-services.html.en

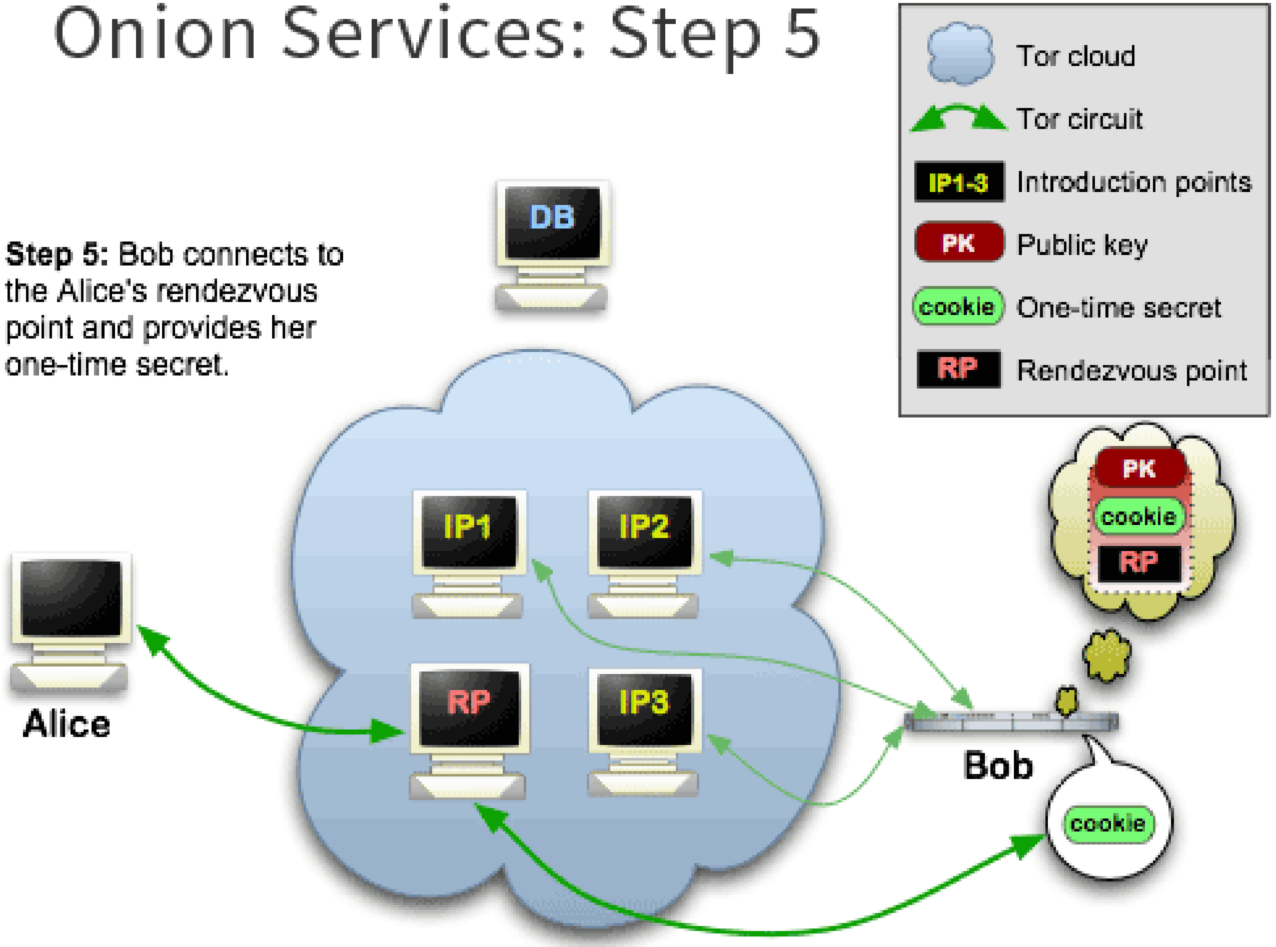
Onion Services: Step 4



Step 4: Alice writes a message to Bob (encrypted to PK) listing the rendezvous point and a one-time secret, and asks an introduction point to deliver it to Bob.

https://www.torproject.org/docs/onion-services.html.en

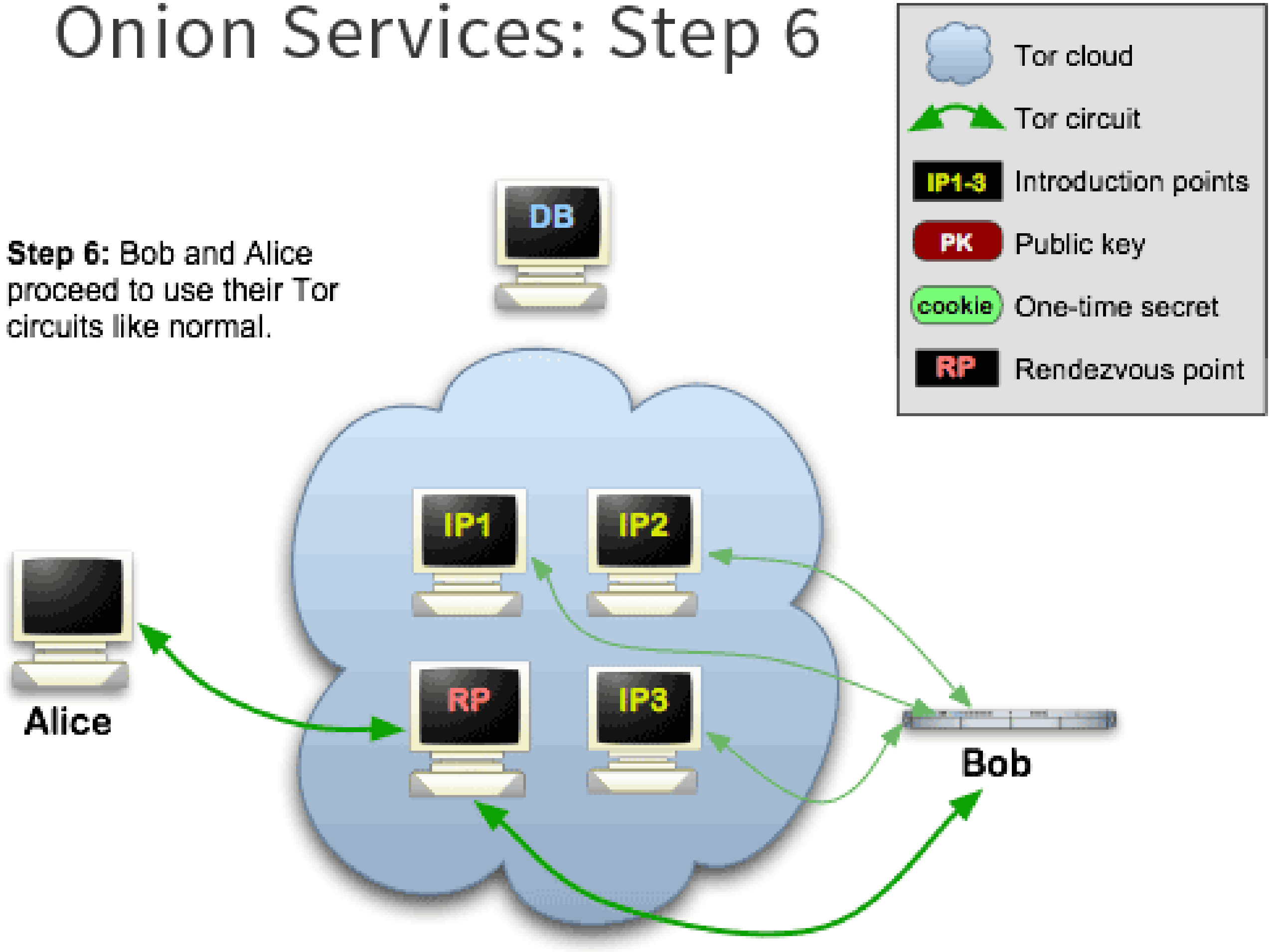
Onion Services: Step 5



Step 5: Bob connects to the Alice's rendezvous point and provides her one-time secret.

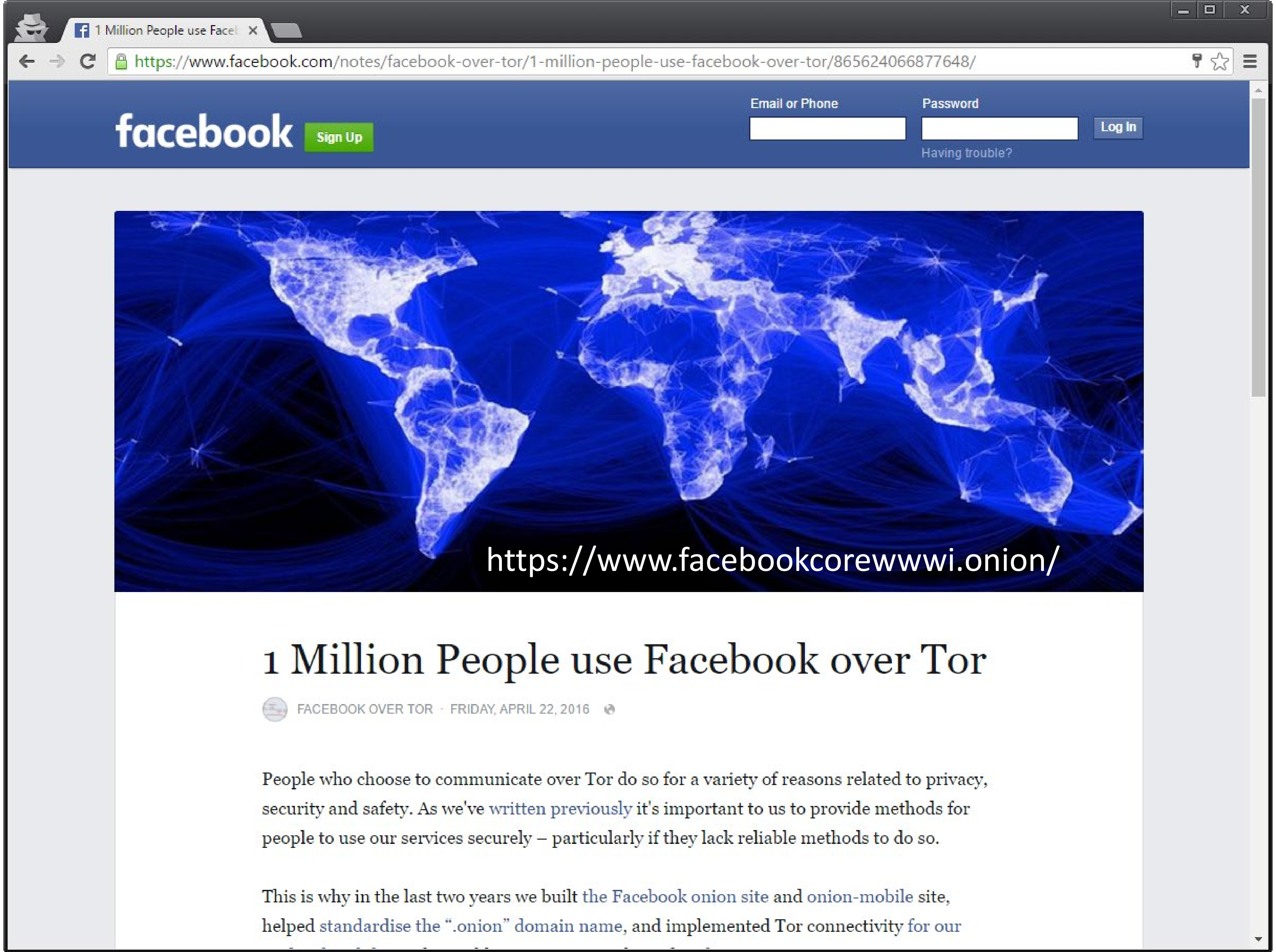
https://www.torproject.org/docs/onion-services.html.en

Onion Services: Step 6



Step 6: Bob and Alice proceed to use their Tor circuits like normal.

https://www.torproject.org/docs/onion-services.html.en



1 Million People use Faceb
https://www.facebook.com/notes/facebook-over-tor/1-million-people-use-facebook-over-tor/865624066877648/
facebook
Sign Up
Email or Phone
Password
Log In
Having trouble?

https://www.facebookcorewwwi.onion/

1 Million People use Facebook over Tor

FACEBOOK OVER TOR · FRIDAY, APRIL 22, 2016

People who choose to communicate over Tor do so for a variety of reasons related to privacy, security and safety. As we've written previously it's important to us to provide methods for people to use our services securely – particularly if they lack reliable methods to do so.

This is why in the last two years we built the Facebook onion site and onion-mobile site, helped standardise the ".onion" domain name, and implemented Tor connectivity for our

Censors want to block Tor

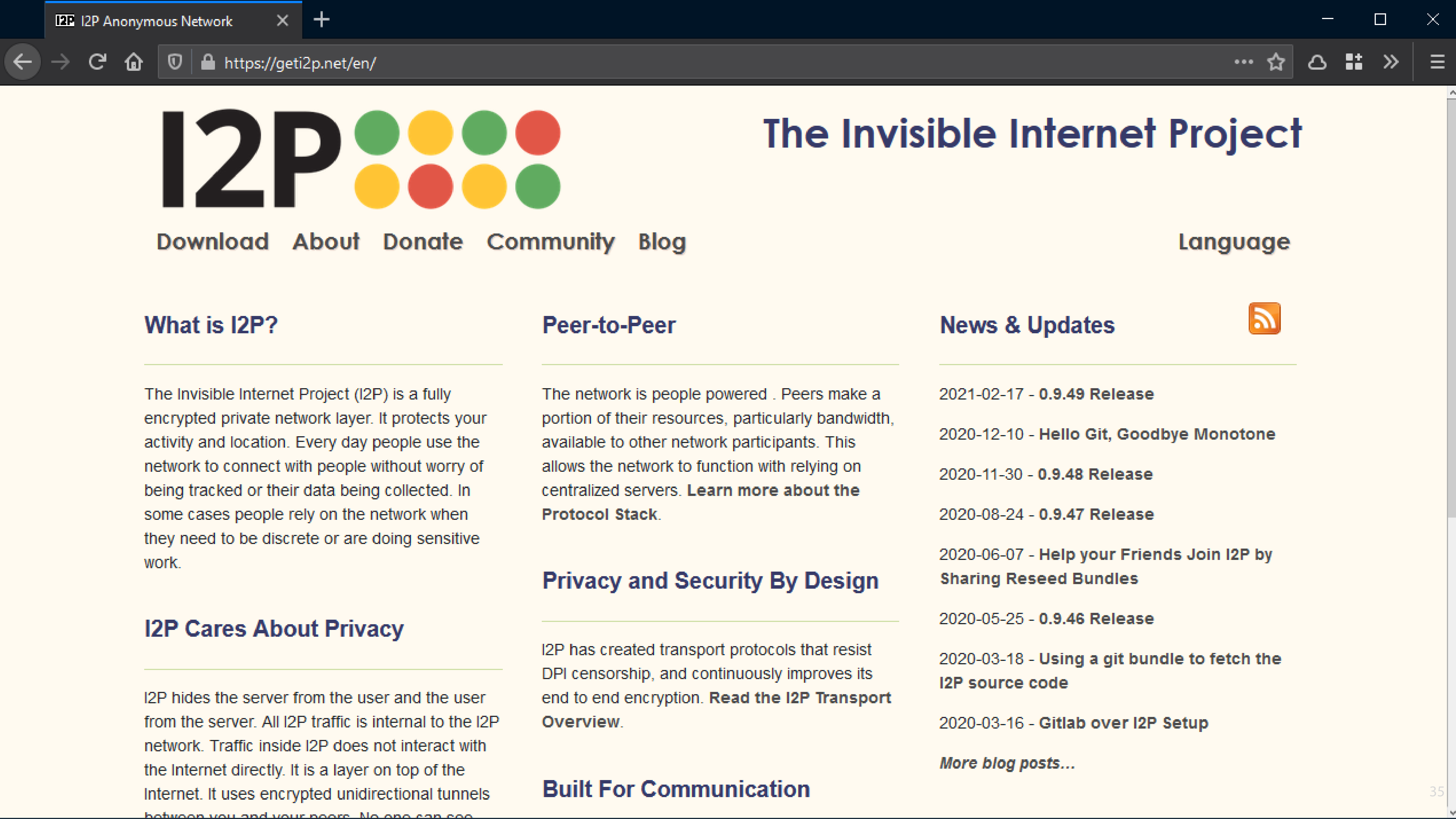
Directory servers are the easy target: just block any access to them

Response: Tor bridges

- Tor relays that aren't listed in the main Tor directory
- Only a few at a time can be obtained on-demand (e.g., through email to bridges@bridges.torproject.org)
- Once known, adversaries may block them too…

Pluggable Transports

- Censors may drop all Tor traffic through deep packet inspection
- Hide Tor traffic in plain sight by masquerading it as some other innocent-looking protocol (HTTP, Skype, Starcraft, …)



I2P The Invisible Internet Project

Download About Donate Community Blog Language

What is I2P?

The Invisible Internet Project (I2P) is a fully encrypted private network layer. It protects your activity and location. Every day people use the network to connect with people without worry of being tracked or their data being collected. In some cases people rely on the network when they need to be discrete or are doing sensitive work.

I2P Cares About Privacy

I2P hides the server from the user and the user from the server. All I2P traffic is internal to the I2P network. Traffic inside I2P does not interact with the Internet directly. It is a layer on top of the Internet. It uses encrypted unidirectional tunnels

Peer-to-Peer

The network is people powered . Peers make a portion of their resources, particularly bandwidth, available to other network participants. This allows the network to function with relying on centralized servers. **Learn more about the Protocol Stack**.

Privacy and Security By Design

I2P has created transport protocols that resist DPI censorship, and continuously improves its end to end encryption. **Read the I2P Transport Overview**.

Built For Communication

News & Updates

2021-02-17 - **0.9.49 Release**

2020-12-10 - **Hello Git, Goodbye Monotone**

2020-11-30 - **0.9.48 Release**

2020-08-24 - **0.9.47 Release**

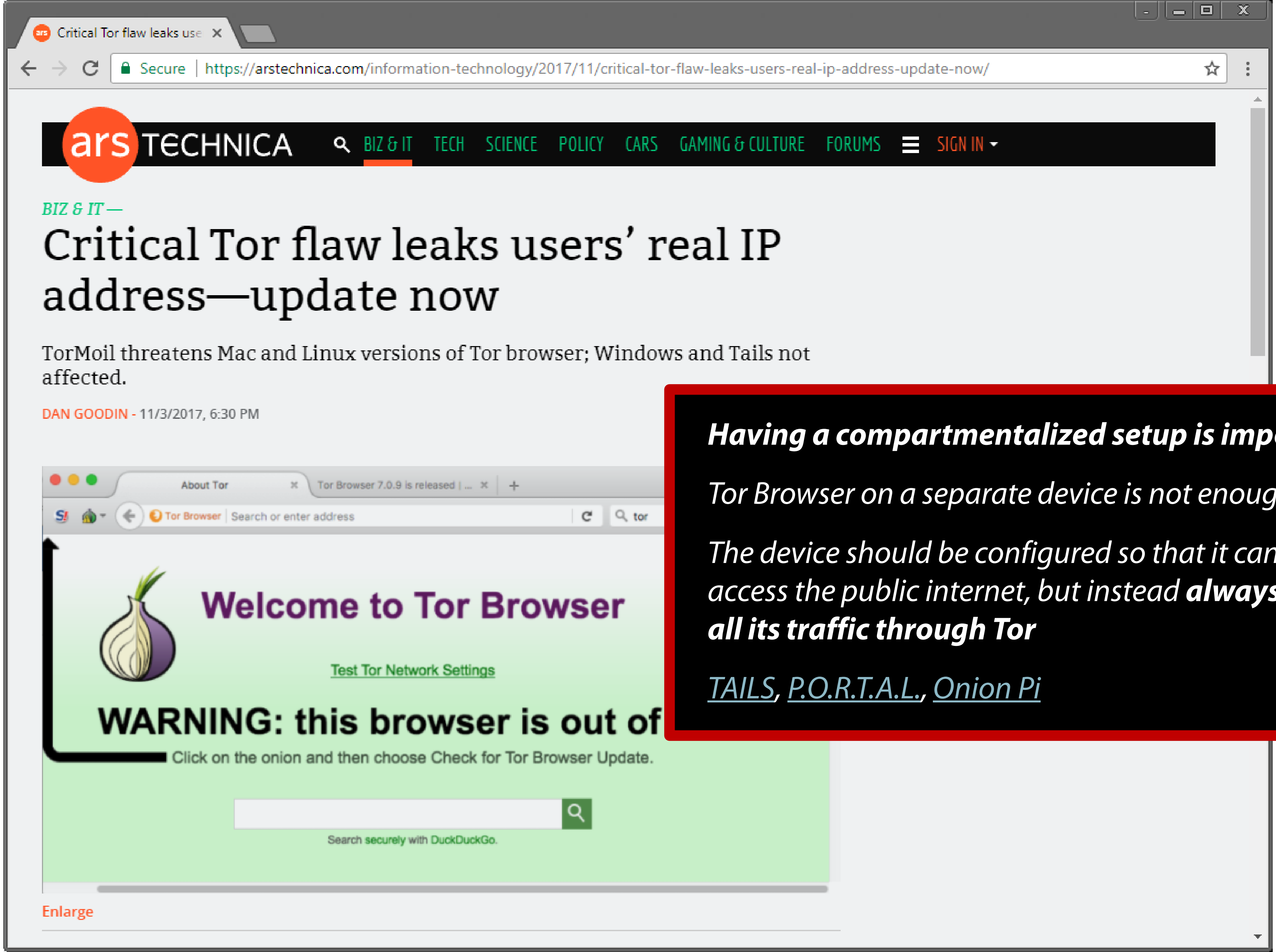
2020-06-07 - **Help your Friends Join I2P by Sharing Reseed Bundles**

2020-05-25 - **0.9.46 Release**

2020-03-18 - **Using a git bundle to fetch the I2P source code**

2020-03-16 - **Gitlab over I2P Setup**

More blog posts...


Critical Tor flaw leaks use
Secure
https://arstechnica.com/information-technology/2017/11/critical-tor-flaw-leaks-users-real-ip-address-update-now/
ars TECHNICA
BIZ & IT
TECH
SCIENCE
POLICY
CARS
GAMING & CULTURE
FORUMS
SIGN IN
About Tor
Tor Browser 7.0.9 is released | ...
Tor Browser
Search or enter address
tor
Test Tor Network Settings
Search securely with DuckDuckGo.
Enlarge

BIZ & IT —

Critical Tor flaw leaks users' real IP address—update now

TorMoil threatens Mac and Linux versions of Tor browser; Windows and Tails not affected.

DAN GOODIN - 11/3/2017, 6:30 PM

Welcome to Tor Browser

WARNING: this browser is out of

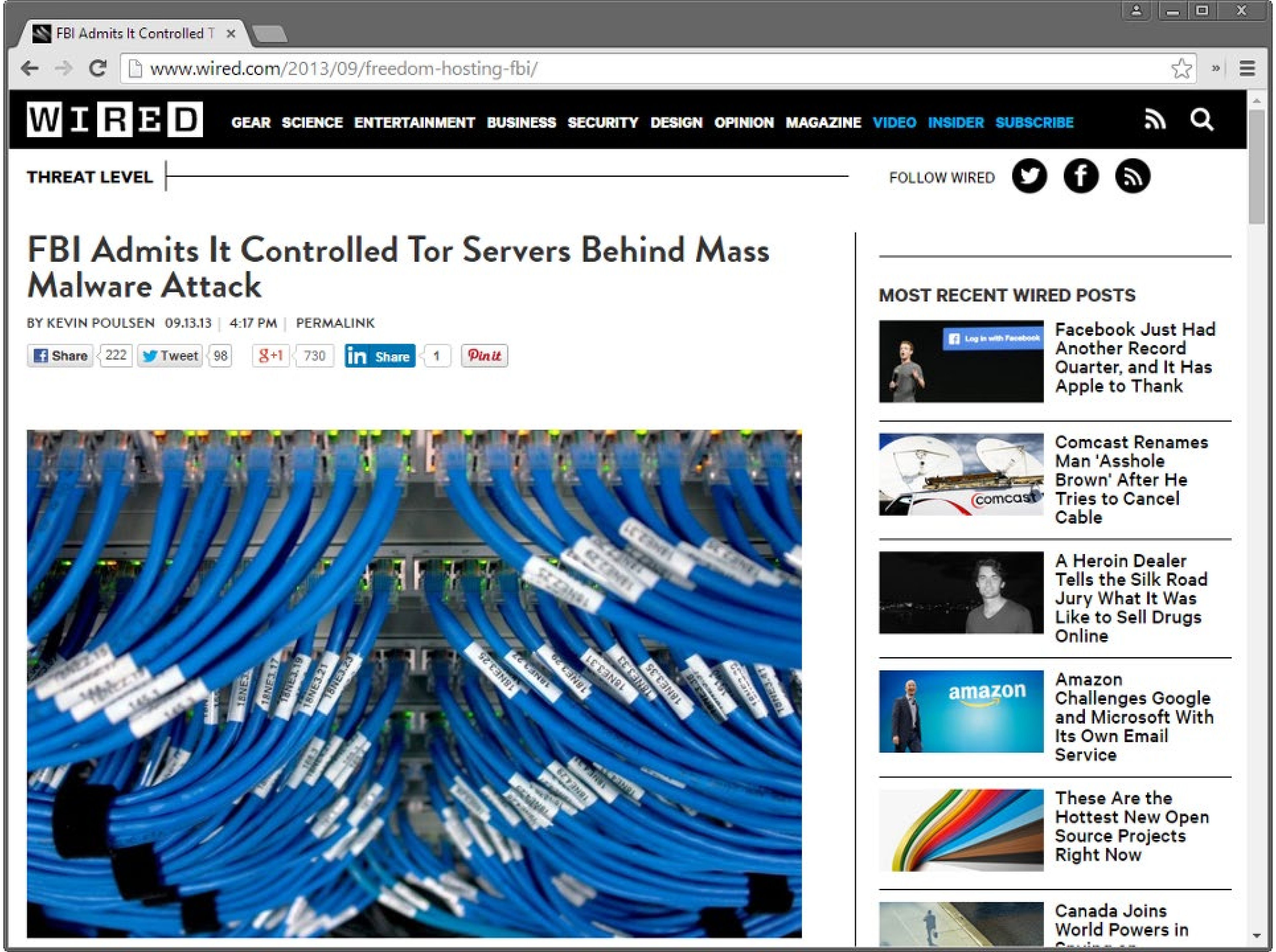
Click on the onion and then choose Check for Tor Browser Update.

Having a compartmentalized setup is important!

Tor Browser on a separate device is not enough

*The device should be configured so that it cannot access the public internet, but instead **always route all its traffic through Tor***

TAILS, P.O.R.T.A.L., Onion Pi



FBI Admits It Controlled T
www.wired.com/2013/09/freedom-hosting-fbi/
WIRED
GEAR SCIENCE ENTERTAINMENT BUSINESS SECURITY DESIGN OPINION MAGAZINE VIDEO INSIDER SUBSCRIBE
THREAT LEVEL
FOLLOW WIRED
Share 222
Tweet 98
g+1 730
in Share 1
Pin it
Log in with Facebook
amazon
comcast

FBI Admits It Controlled Tor Servers Behind Mass Malware Attack

BY KEVIN POULSEN 09.13.13 | 4:17 PM | PERMALINK

MOST RECENT WIRED POSTS

Facebook Just Had Another Record Quarter, and It Has Apple to Thank

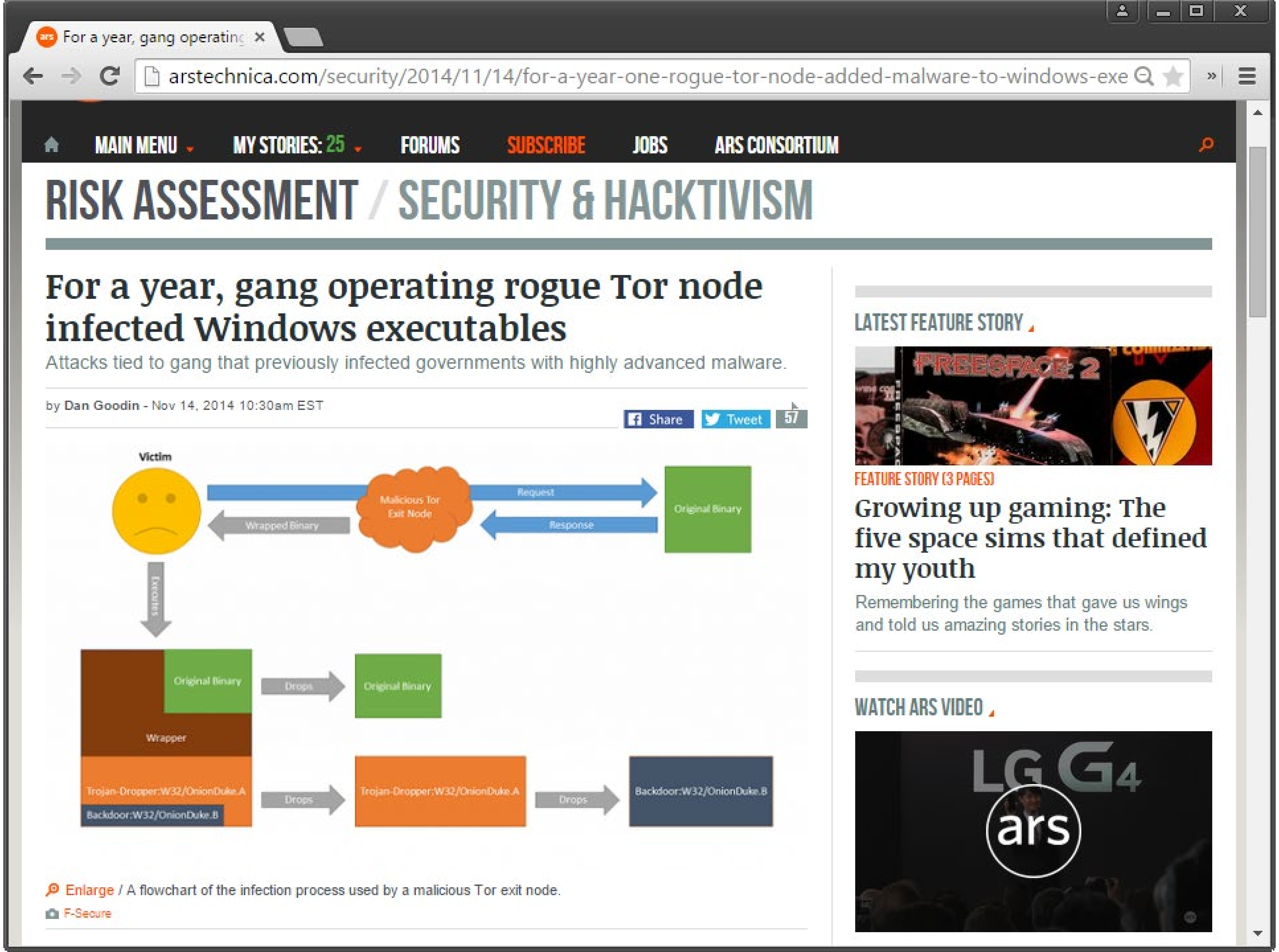
Comcast Renames Man 'Asshole Brown' After He Tries to Cancel Cable

A Heroin Dealer Tells the Silk Road Jury What It Was Like to Sell Drugs Online

Amazon Challenges Google and Microsoft With Its Own Email Service

These Are the Hottest New Open Source Projects Right Now

Canada Joins World Powers in



For a year, gang operatinc ×
arstechnica.com/security/2014/11/14/for-a-year-one-rogue-tor-node-added-malware-to-windows-exe
MAIN MENU
MY STORIES: 25
FORUMS
SUBSCRIBE
JOBS
ARS CONSORTIUM

RISK ASSESSMENT / SECURITY & HACKTIVISM

For a year, gang operating rogue Tor node infected Windows executables

Attacks tied to gang that previously infected governments with highly advanced malware.

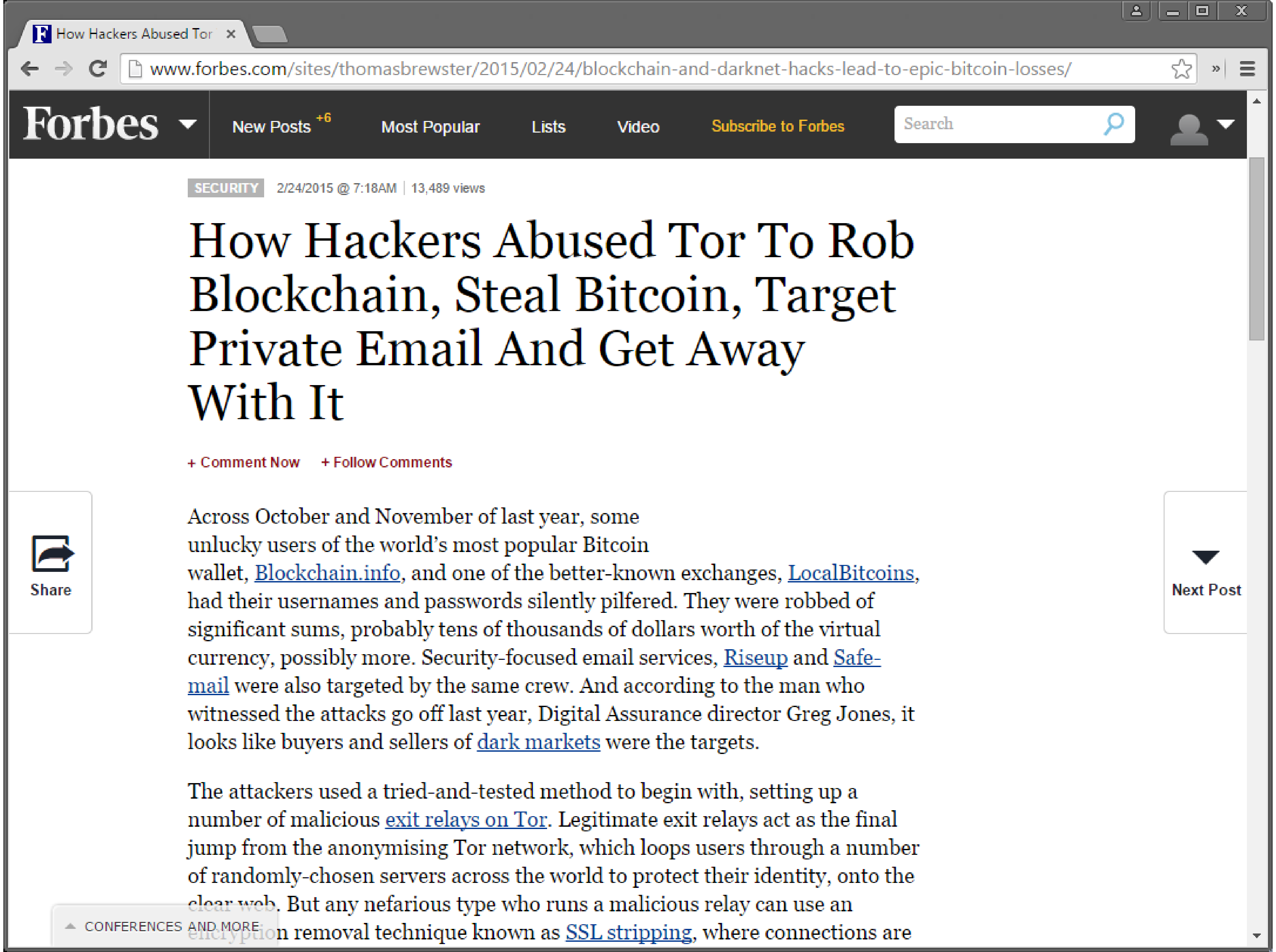
by Dan Goodin - Nov 14, 2014 10:30am EST

Enlarge / A flowchart of the infection process used by a malicious Tor exit node.

F-Secure

Growing up gaming: The five space sims that defined my youth

Remembering the games that gave us wings and told us amazing stories in the stars.



SECURITY 2/24/2015 @ 7:18AM | 13,489 views

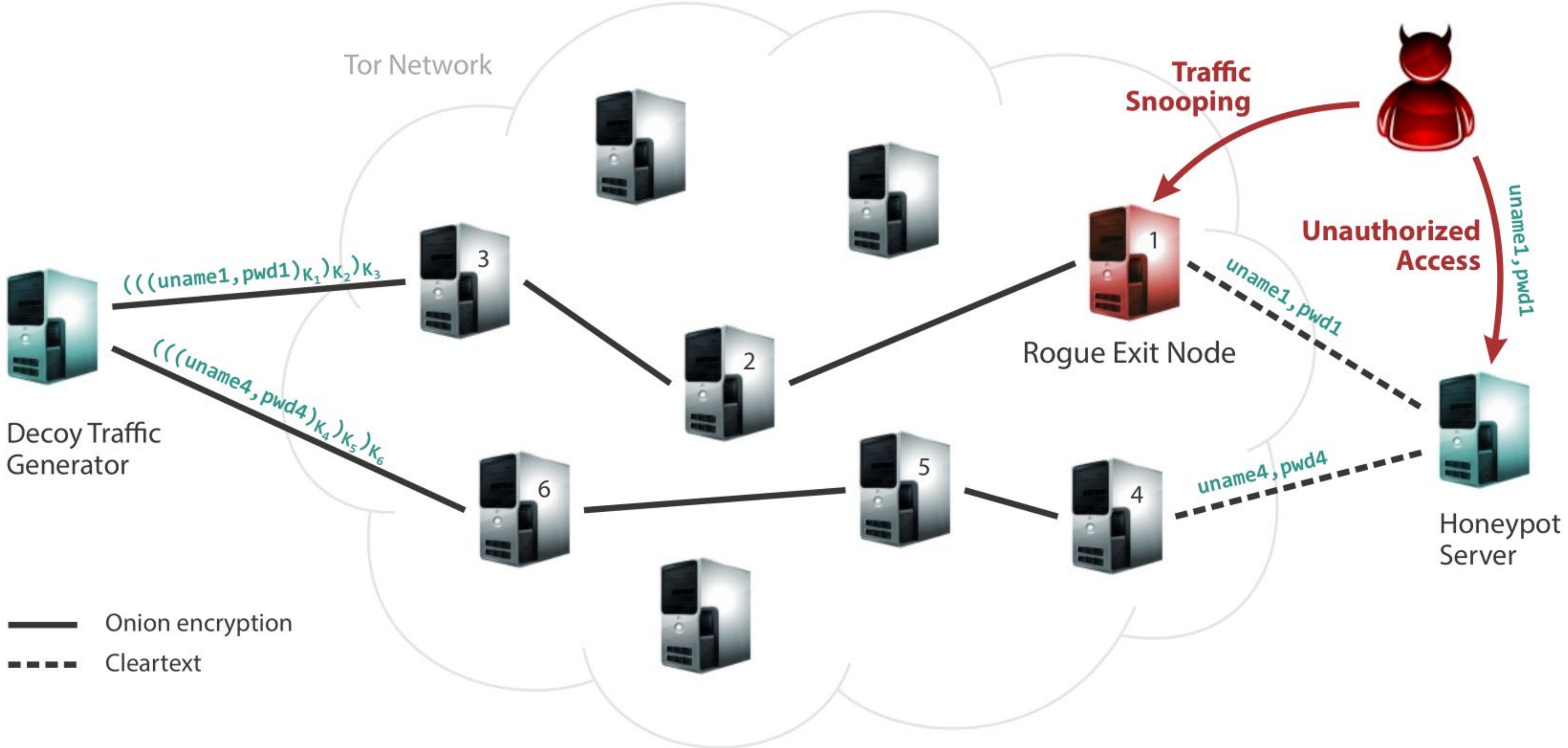
How Hackers Abused Tor To Rob Blockchain, Steal Bitcoin, Target Private Email And Get Away With It

+ Comment Now + Follow Comments

Across October and November of last year, some unlucky users of the world's most popular Bitcoin wallet, Blockchain.info, and one of the better-known exchanges, LocalBitcoins, had their usernames and passwords silently pilfered. They were robbed of significant sums, probably tens of thousands of dollars worth of the virtual currency, possibly more. Security-focused email services, Riseup and Safe-mail were also targeted by the same crew. And according to the man who witnessed the attacks go off last year, Digital Assurance director Greg Jones, it looks like buyers and sellers of dark markets were the targets.

The attackers used a tried-and-tested method to begin with, setting up a number of malicious exit relays on Tor. Legitimate exit relays act as the final jump from the anonymising Tor network, which loops users through a number of randomly-chosen servers across the world to protect their identity, onto the clear web. But any nefarious type who runs a malicious relay can use an encryption removal technique known as SSL stripping, where connections are

Detecting Traffic Snooping in Tor using Decoys

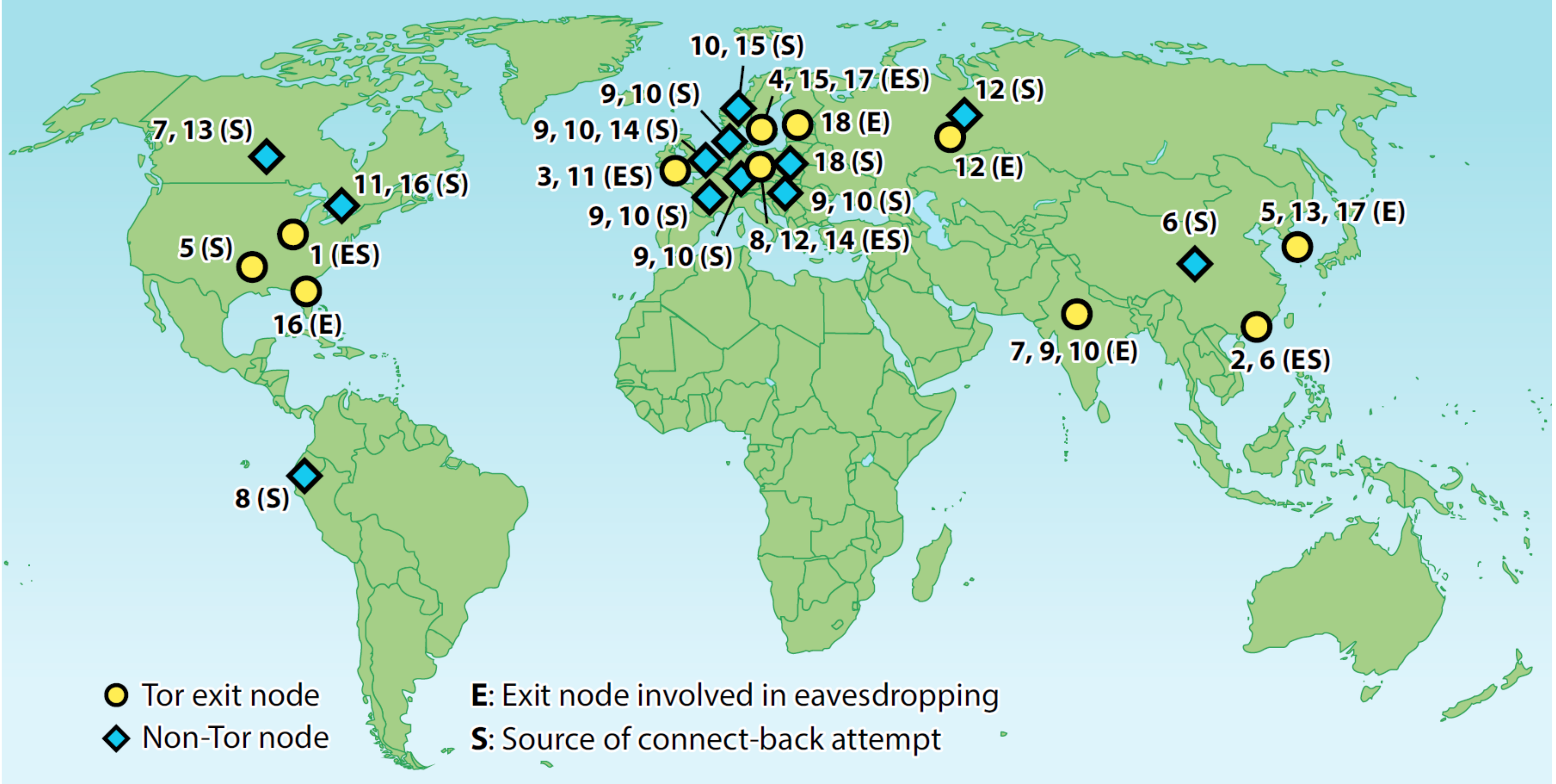


Expose unique decoy username+password through each exit node

Wait for unsolicited connections to the honeypot server using any of the exposed bait credentials

Detecting Traffic Snooping in Tor Using Decoys – RAID 2011

Detected Rogue Exit Nodes



30-month period: detected **18 cases** of traffic eavesdropping that involved **14 different Tor exit nodes**

Online Privacy and Anonymity: What Can We do?

Technical solutions exist

- End-to-end encryption
- Self-hosted services
- Anonymous communication
- …

But they are not enough

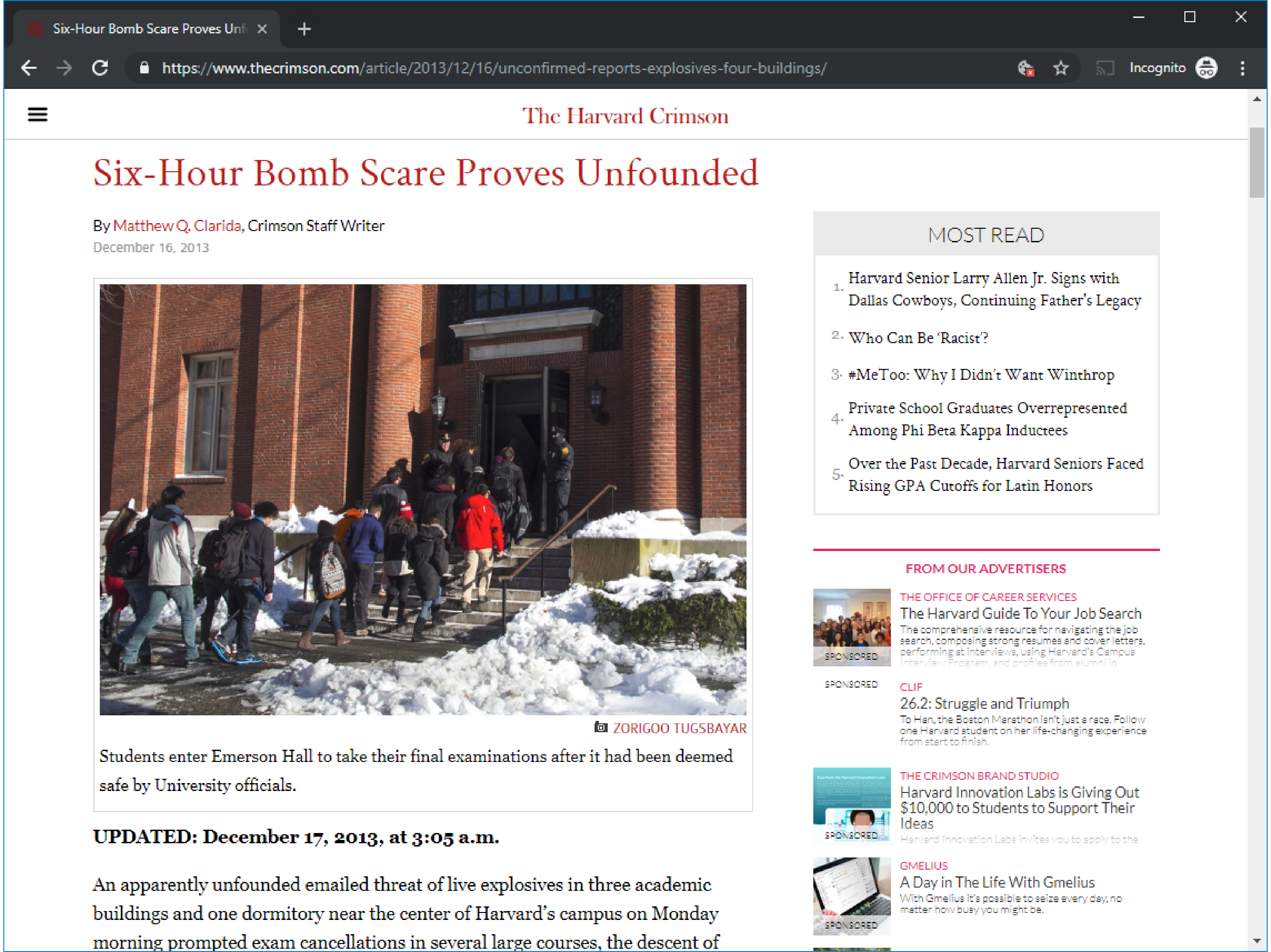
- Privacy vs. usability tradeoff
- Wrong assumptions
- Implementation flaws

Many users are not even aware of privacy issues, let alone solutions

Protect the right of individuals to control what information may be collected

- *With technical means, not promises…*

Case (Failure) Studies



Six-Hour Bomb Scare Proves Unf ×
+
https://www.thecrimson.com/article/2013/12/16/unconfirmed-reports-explosives-four-buildings/
Incognito

The Harvard Crimson

Six-Hour Bomb Scare Proves Unfounded

By Matthew Q. Clarida, Crimson Staff Writer
December 16, 2013

ZORIGOO TUGSBAYAR

Students enter Emerson Hall to take their final examinations after it had been deemed safe by University officials.

UPDATED: December 17, 2013, at 3:05 a.m.

An apparently unfounded emailed threat of live explosives in three academic buildings and one dormitory near the center of Harvard's campus on Monday morning prompted exam cancellations in several large courses, the descent of

MOST READ

1. Harvard Senior Larry Allen Jr. Signs with Dallas Cowboys, Continuing Father's Legacy
2. Who Can Be 'Racist'?
3. #MeToo: Why I Didn't Want Winthrop
4. Private School Graduates Overrepresented Among Phi Beta Kappa Inductees
5. Over the Past Decade, Harvard Seniors Faced Rising GPA Cutoffs for Latin Honors

Case Study: Bomb Threat at Harvard University

Strategic objective: avoid final exam

- Cause an evacuation of the building where the exam would take place

Operation plan:

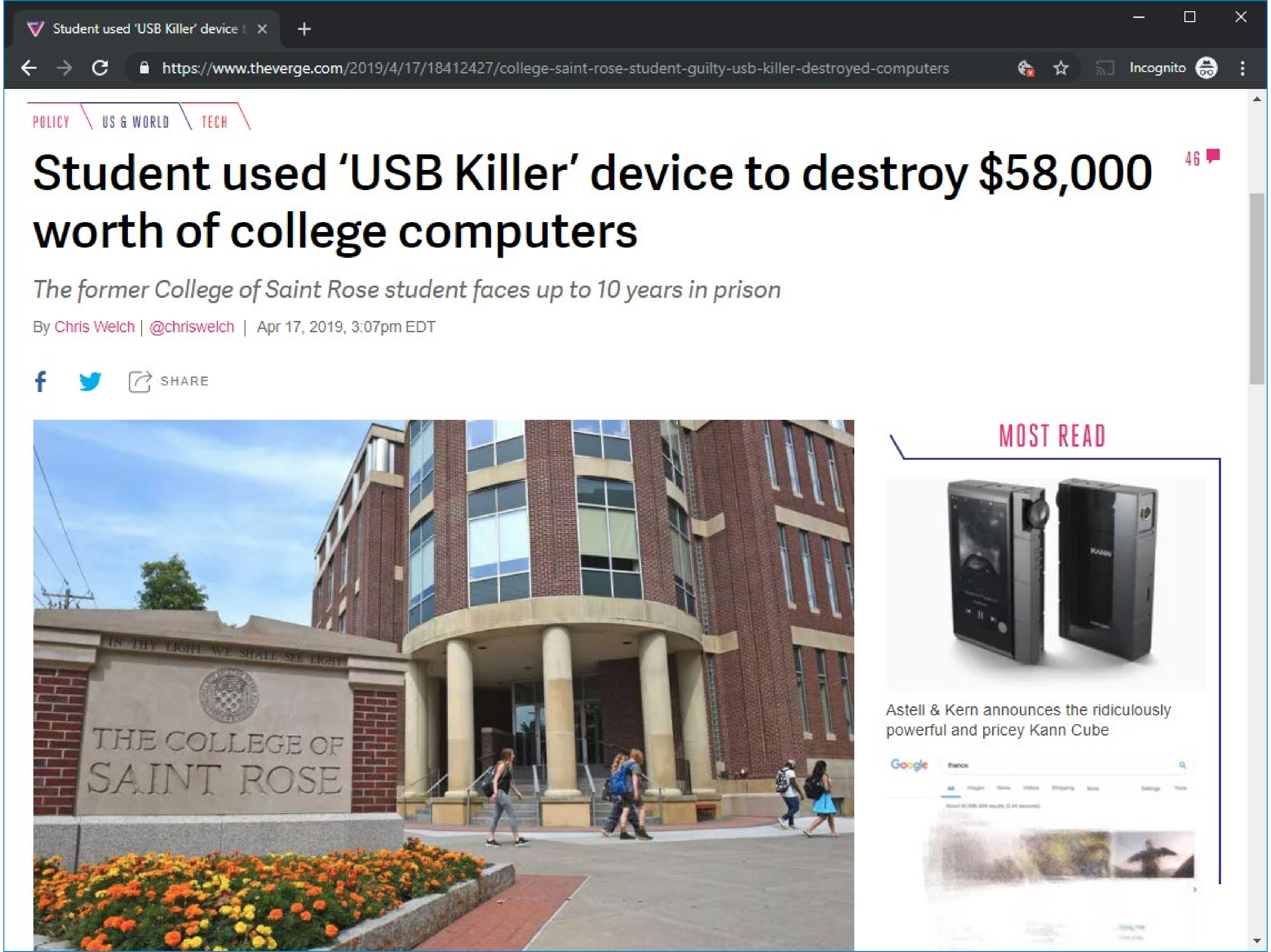
- Tor Browser Bundle
- Compose email *(“bombs placed in science center, server hall, …”)*
- For each target email address, send message using a new disposable `guerrillamail.com` account

Fatal error: used the Harvard University WiFi network

- Had to login with his username and password
- His IP was used to access Tor, and this information was logged
- Pool of suspects immediately reduced to “everyone that used Tor during the time the bomb threats were sent”

© The Grugq - http://grugq.github.io/blog/2013/12/21/in-search-of-opsec-magic-sauce/

Tor protects you but also makes you stick out


Student used 'USB Killer' device t
https://www.theverge.com/2019/4/17/18412427/college-saint-rose-student-guilty-usb-killer-destroyed-computers
Incognito
POLICY
US & WORLD
TECH
46
SHARE
IN THY LIGHT WE SHALL SEE LIGHT
THE COLLEGE OF SAINT ROSE
MOST READ
Google
thanos

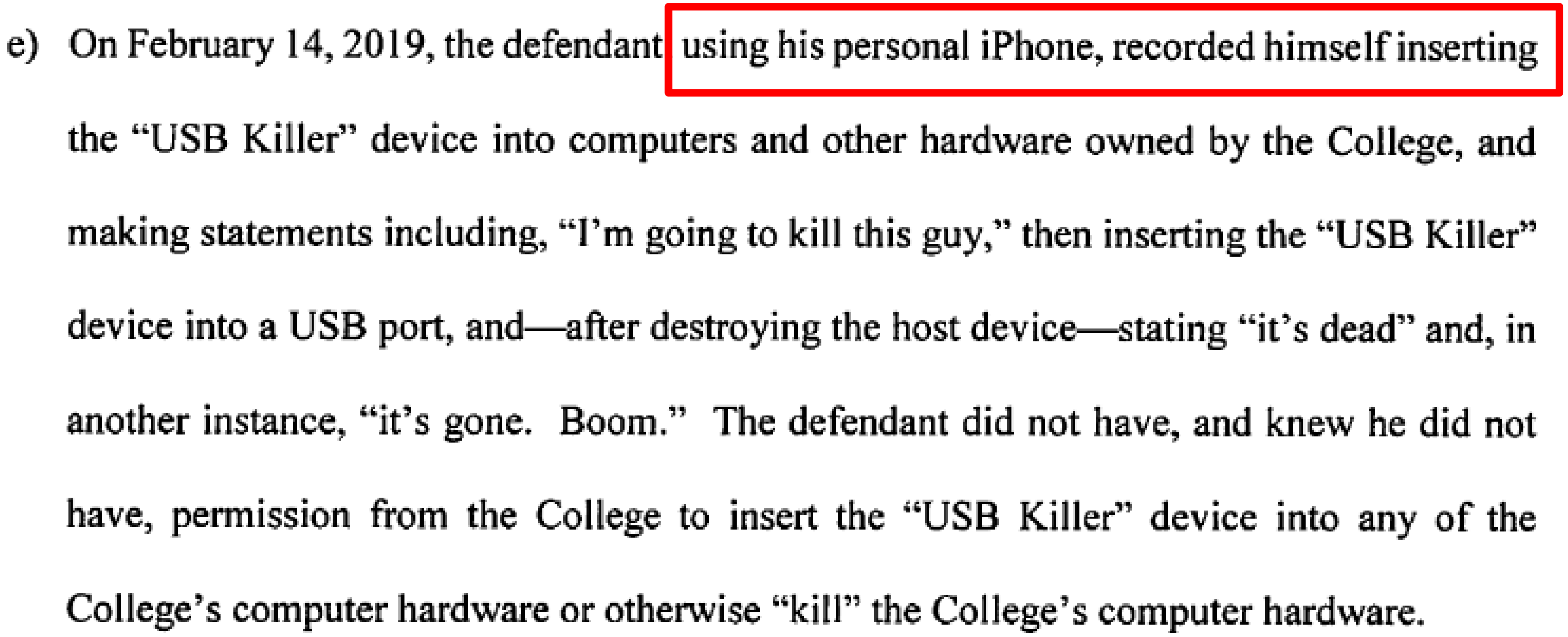
Student used 'USB Killer' device to destroy $58,000 worth of college computers

The former College of Saint Rose student faces up to 10 years in prison

By Chris Welch | @chriswelch | Apr 17, 2019, 3:07pm EDT

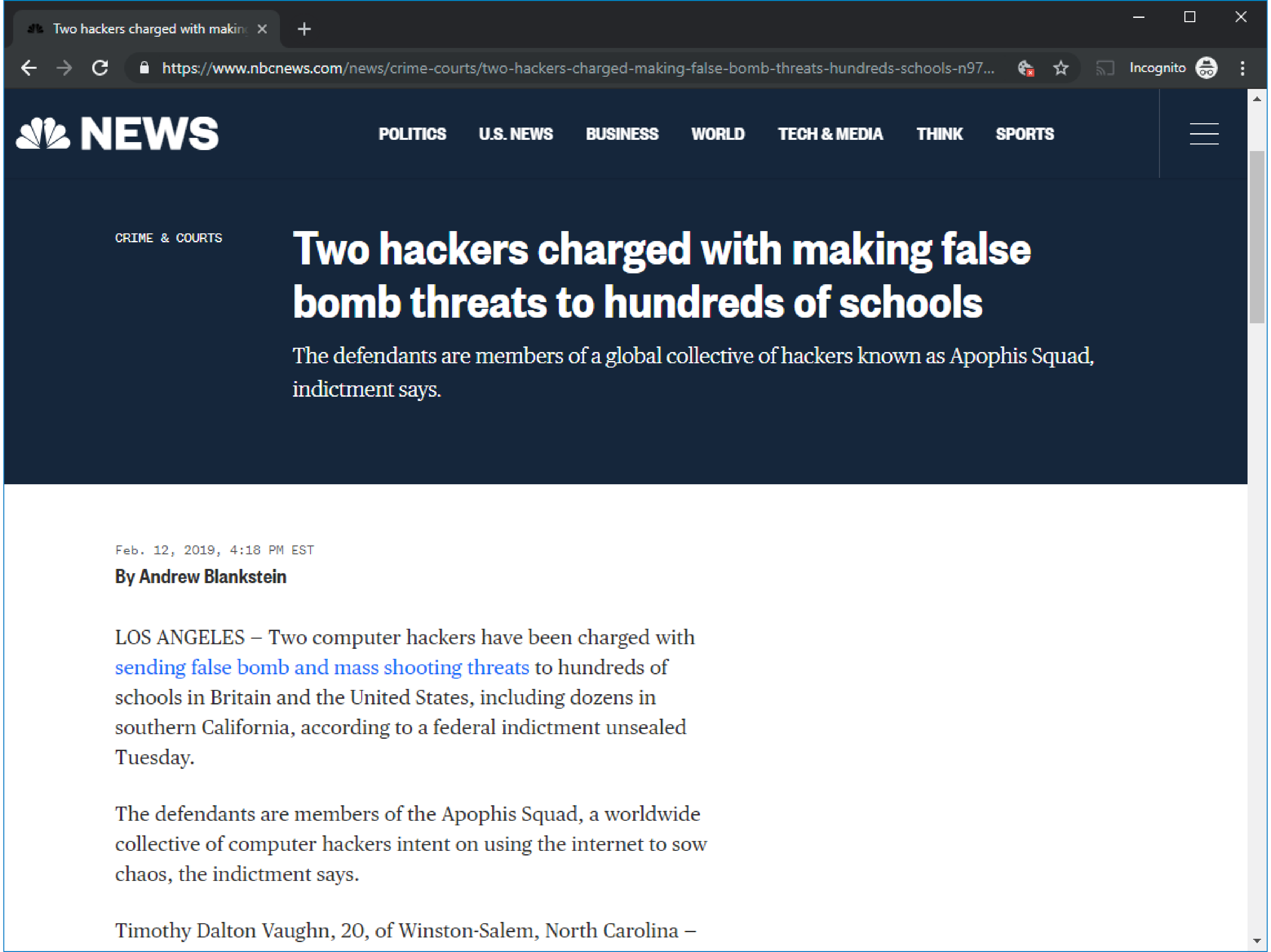
Astell & Kern announces the ridiculously powerful and pricey Kann Cube

Case Study: USB Killer Damage



e) On February 14, 2019, the defendant using his personal iPhone, recorded himself inserting the "USB Killer" device into computers and other hardware owned by the College, and making statements including, "I'm going to kill this guy," then inserting the "USB Killer" device into a USB port, and—after destroying the host device—stating "it's dead" and, in another instance, "it's gone. Boom." The defendant did not have, and knew he did not have, permission from the College to insert the "USB Killer" device into any of the College's computer hardware or otherwise "kill" the College's computer hardware.

Don’t record yourself while conducting a crime


Two hackers charged with makin
https://www.nbcnews.com/news/crime-courts/two-hackers-charged-making-false-bomb-threats-hundreds-schools-n97...
Incognito
NEWS
POLITICS
U.S. NEWS
BUSINESS
WORLD
TECH & MEDIA
THINK
SPORTS

CRIME & COURTS

Two hackers charged with making false bomb threats to hundreds of schools

The defendants are members of a global collective of hackers known as Apophis Squad, indictment says.

Feb. 12, 2019, 4:18 PM EST

By Andrew Blankstein

LOS ANGELES – Two computer hackers have been charged with sending false bomb and mass shooting threats to hundreds of schools in Britain and the United States, including dozens in southern California, according to a federal indictment unsealed Tuesday.

The defendants are members of the Apophis Squad, a worldwide collective of computer hackers intent on using the internet to sow chaos, the indictment says.

Timothy Dalton Vaughn, 20, of Winston-Salem, North Carolina –

Case Study: Bomb Threats

Vaughn used multiple aliases on Twitter and elsewhere to brag about his attacks, including "HDGZero"

- Doing pretty OK, LEAs could not track him down

January 2019: game company BlankMediaGames got breached

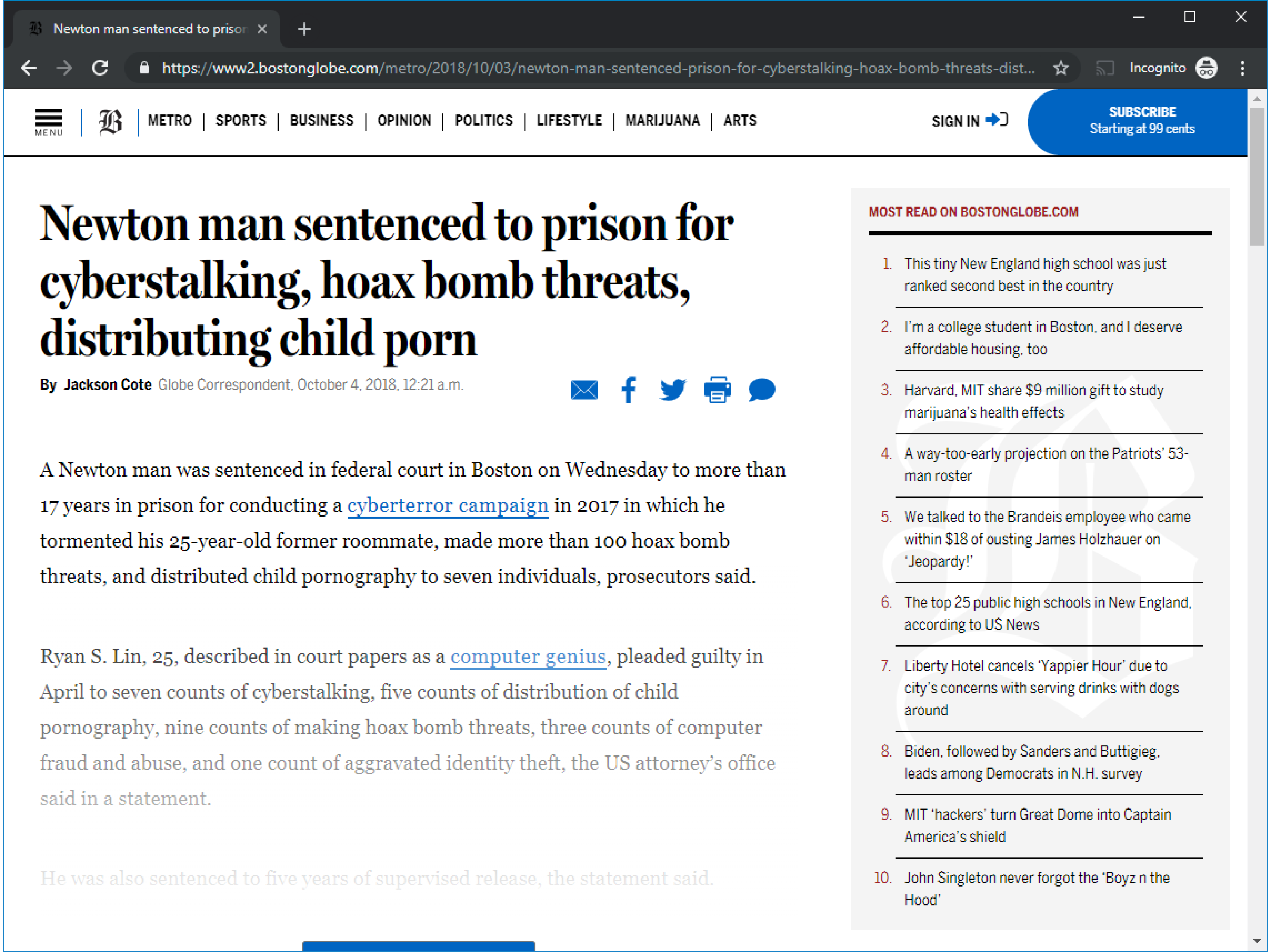
- Leaked accounts of 7.6 million people signed up to play the game "Town of Salem" started circulating

Leaked DB contained an interesting 2018 entry:

- Username: `hdgzero`
- Email address: `xavierfarbel@gmail.com`
- Account registered using a Sprint mobile device that had an IP address originating from the Carolinas

https://krebsonsecurity.com/2019/02/bomb-threat-hoaxer-exposed-by-hacked-gaming-site/

Avoid contamination



Newton man sentenced to prison
https://www2.bostonglobe.com/metro/2018/10/03/newton-man-sentenced-prison-for-cyberstalking-hoax-bomb-threats-dist...
Incognito
MENU
METRO | SPORTS | BUSINESS | OPINION | POLITICS | LIFESTYLE | MARIJUANA | ARTS
SIGN IN
SUBSCRIBE
Starting at 99 cents

Newton man sentenced to prison for cyberstalking, hoax bomb threats, distributing child porn

By Jackson Cote Globe Correspondent, October 4, 2018, 12:21 a.m.

A Newton man was sentenced in federal court in Boston on Wednesday to more than 17 years in prison for conducting a cyberterror campaign in 2017 in which he tormented his 25-year-old former roommate, made more than 100 hoax bomb threats, and distributed child pornography to seven individuals, prosecutors said.

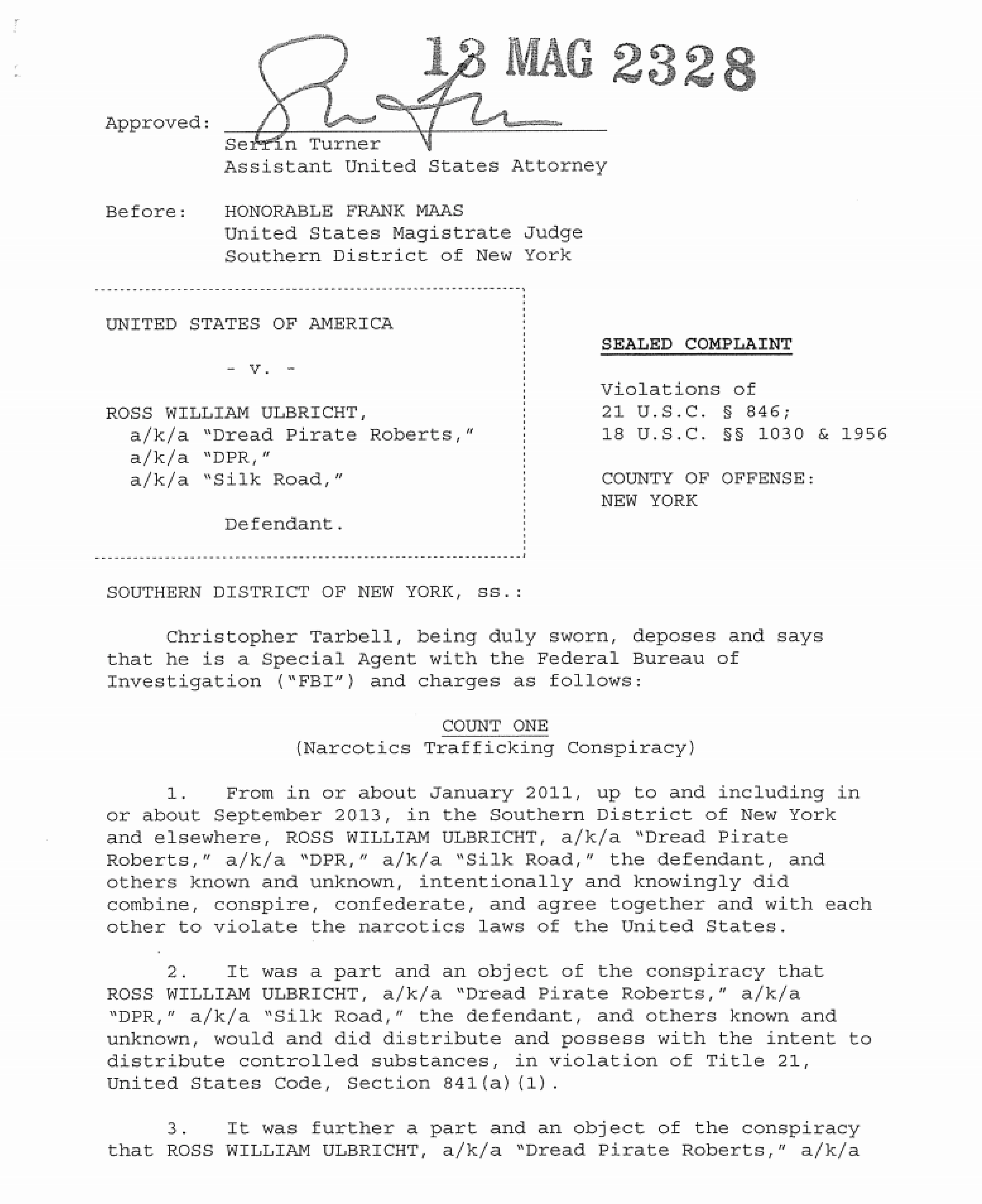
Ryan S. Lin, 25, described in court papers as a computer genius, pleaded guilty in April to seven counts of cyberstalking, five counts of distribution of child pornography, nine counts of making hoax bomb threats, three counts of computer fraud and abuse, and one count of aggravated identity theft, the US attorney's office said in a statement.

He was also sentenced to five years of supervised release, the statement said.

Case Study: Cyberstalking

- Lin took measures to mask his identity
  - Tor, ProtonMail anonymous email account, VPN services
- Former employer provided Lin’s work computer
  - Had been formatted ➔ forensic extraction of data
  - Found links to ProtonMail account, victims’ online profiles, …
- Artifacts suggesting the use of PureVPN and WANSecurity VPN services
  - LEAs obtained connection logs from both companies
  - PureVPN was accessed from both home and work
  - Used the same VPN accounts to access both his real accounts and the fake profiles he created to harass victims

Avoid relying solely on VPNs



13 MAG 2328

Approved: ________________________________
Serrin Turner
Assistant United States Attorney

Before: HONORABLE FRANK MAAS
United States Magistrate Judge
Southern District of New York

UNITED STATES OF AMERICA

- v. -

ROSS WILLIAM ULBRICHT,
a/k/a "Dread Pirate Roberts,"
a/k/a "DPR,"
a/k/a "Silk Road,"

Defendant.

SEALED COMPLAINT

Violations of
21 U.S.C. § 846;
18 U.S.C. §§ 1030 & 1956

COUNTY OF OFFENSE:
NEW YORK

SOUTHERN DISTRICT OF NEW YORK, ss.:

Christopher Tarbell, being duly sworn, deposes and says that he is a Special Agent with the Federal Bureau of Investigation ("FBI") and charges as follows:

COUNT ONE
(Narcotics Trafficking Conspiracy)

1. From in or about January 2011, up to and including in or about September 2013, in the Southern District of New York and elsewhere, ROSS WILLIAM ULBRICHT, a/k/a "Dread Pirate Roberts," a/k/a "DPR," a/k/a "Silk Road," the defendant, and others known and unknown, intentionally and knowingly did combine, conspire, confederate, and agree together and with each other to violate the narcotics laws of the United States.

2. It was a part and an object of the conspiracy that ROSS WILLIAM ULBRICHT, a/k/a "Dread Pirate Roberts," a/k/a "DPR," a/k/a "Silk Road," the defendant, and others known and unknown, would and did distribute and possess with the intent to distribute controlled substances, in violation of Title 21, United States Code, Section 841(a)(1).

3. It was further a part and an object of the conspiracy that ROSS WILLIAM ULBRICHT, a/k/a "Dread Pirate Roberts," a/k/a

Case Study: Silk Road

Fail #1 [Jan 2011]: two forum posts on shroomery.org and Bitcoin Talk

- Both by user `altoid`
- Among the first to advertise a hidden Tor service that operated as a kind of *"anonymous amazon.com"*
- Both posts referenced `silkroad420.wordpress.com`

Fail #2 [Oct 2011]: post by user `altoid` on Bitcoin Talk

- Titled *"a venture backed Bitcoin startup company"*
- Looking for an *"IT pro in the Bitcoin community"*
- Directed interested users to `rossulbricht@gmail.com`

Link: Silk Road ➔ altoid ➔ rossulbricht@gmail.com

https://grugq.tumblr.com/post/62914009002/silk-road-investigation-timeline

Case Study: Silk Road

Fail #3: `rossulbricht@gmail.com` Google+ profile

- Included a list of favorite videos originating from mises.org
- Website of the Mises Institute (the "world center of the Austrian School of economics")
- Site contained a user profile for one Ross Ulbricht

Several Dread Pirate Roberts postings on Silk Road cited the "Austrian Economic theory"

- Including works of the Institute's economists Ludwig von Mises and Murray Rothbard
- Provided the guiding principles for the illicit drug market

(Soft) Link: Ross Ulbricht ➔ Silk Road

https://grugq.tumblr.com/post/62914009002/silk-road-investigation-timeline

Case Study: Silk Road

Fail #4 [March 2012]: new account on StackOverflow

Username: `Ross Ulbricht`

Email address: `rossulbricht@gmail.com`

[March 16]: *"How can I connect to a Tor hidden service using curl in php"*

[1 minute later]: username changed from `Ross Ulbricht` to `frosty`

[weeks later]: account updated again, Gmail address changed to `frosty@frosty.com`

Link: Ross Ulbricht ➔ frosty

https://grugq.tumblr.com/post/62914009002/silk-road-investigation-timeline

Case Study: Silk Road

Fail #5: Server IP address leakage

Reddit thread: A user posted a warning that Silk Road's IP address was "leaking"

FBI saw it and started fiddling with Silk Road's login page until it leaked its public IP address

- When they entered the leaked IP address directly into a browser, Silk Road's CAPTCHA prompt appeared

Main server was located in a data center in Iceland

- Reykjavik police accessed and secretly copied the server's data

Tor hidden service busted ➔ beginning of the end

https://grugq.tumblr.com/post/62914009002/silk-road-investigation-timeline

Case Study: Silk Road

Fail #6: SSH

The server's `~/.ssh/authorized_keys` file contained a public SSH key with username `frosty@frosty.com`

By googling around for content like "frosty Tor" the FBI discovered the StackOverflow post

Link: Ross Ulbricht ➔ frosty@frosty.com ➔ Silk Road

https://grugq.tumblr.com/post/62914009002/silk-road-investigation-timeline

Case Study: Silk Road

Fail #7: Location leakage

Remote server administration: Home ➔ VPN ➔ Silk Road server

- Non-Tor path (!)

The server image contained the IP address of the VPN server Ulbricht was logging in from

- The hosting provider gave up the access records for the VPN server to the FBI
- Last login on the VPN server was from Café Luna, San Francisco
- Ulbricht’s home was half a block away
- Matched the location in Google’s records of the account used for the forum posts (both activities happened on the same day)

https://grugq.tumblr.com/post/62914009002/silk-road-investigation-timeline

Case Study: Silk Road

Fail #8 [July 2013]: Fake IDs

US customs intercepts package from Canada

- Contained nine fake IDs, all under different names
- All having the same (real) picture of Ross Ulbricht
- Package was addressed to Ulbricht's San Francisco apartment

Homeland Security was dispatched to the address and found Ulbricht on the spot

- Ulbricht told authorities that someone must have targeted him
- *‘hypothetically’ anyone could go to a website named ‘Silk Road’ on ‘Tor’ and purchase any drugs or fake identity documents*

https://grugq.tumblr.com/post/62914009002/silk-road-investigation-timeline

Avoid contamination

Avoid sending illegal items to your home

Avoid putting your face on fake IDs for online use

Avoid using servers located in MLAT countries

Avoid PHP

Happy Hacking!