Tor Anonymity Network

Tom Ryder
tom@sanctum.geek.nz
https://sanctum.geek.nz/

DISCLAIMER

Use of Tor itself is legal, *but*:

- Please don’t harm others—or your own soul.
- Anything you do with Tor is your own responsibility.
- Smart people still get caught—see Ross Ulbricht.

I know none of you folks are like this, but I’m going to put these slides on my website later.

What is Tor?

Tor is an **anonymity network**, to help you use the internet **anonymously** or (more generally) to protect your **privacy** while using the internet.

It is free and open-source software.

What is the Tor Browser Bundle?

The **Tor Browser Bundle** is a customized version of Firefox configured to use the Tor anonymity network for private and anonymous **web browsing**.

Like Tor—and Firefox itself—it is free and open-source software.

Surveillance—“the old normal”

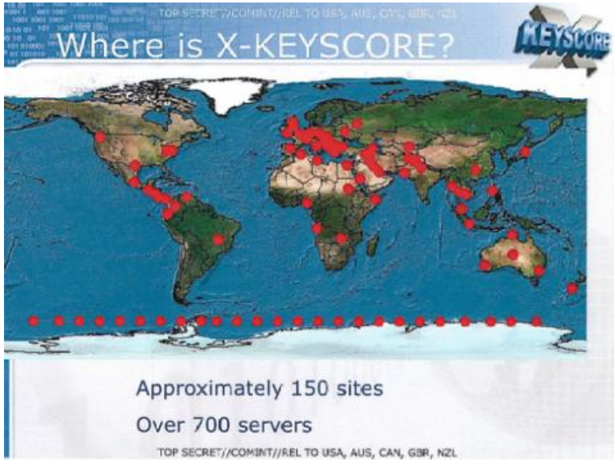
- **Edward Snowden** revealed global surveillance on a massive scale in 2013.
- The **NSA** and the **Five Eyes** (USA, CA, UK, AU, NZ) were the focus of the leaks.
- Whatever you think of Snowden, you now know—you can be watched!

XKeyscore—“whenever, wherever”

Massive NSA data-retrieval system—user interfaces, databases, servers, software…

“You could read **anyone’s email in the world**, anybody you've got an email address for. Any website: **you can watch traffic to and from it**. Any computer that an individual sits at: **you can watch it**. Any laptop that you're tracking: **you can follow it** as it moves from place to place throughout the world.”

—Edward Snowden, 2016 (emphasis mine)



TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Where is X-KEYSCORE?

Approximately 150 sites

Over 700 servers

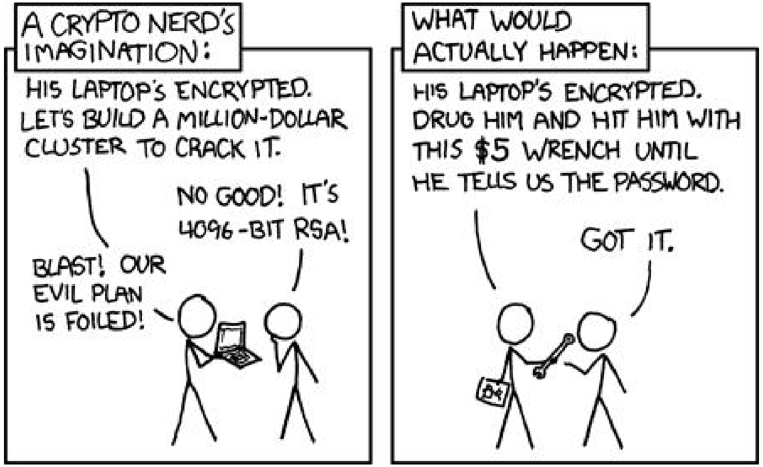
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Dragnet vs Targeted—1/2

- The capabilities of XKeyscore as described by Snowden are **targeted**.
- They seem to be be best used when you *already know* who you’re looking for.
- And if you’re really a person of interest, there’s not much you can do…

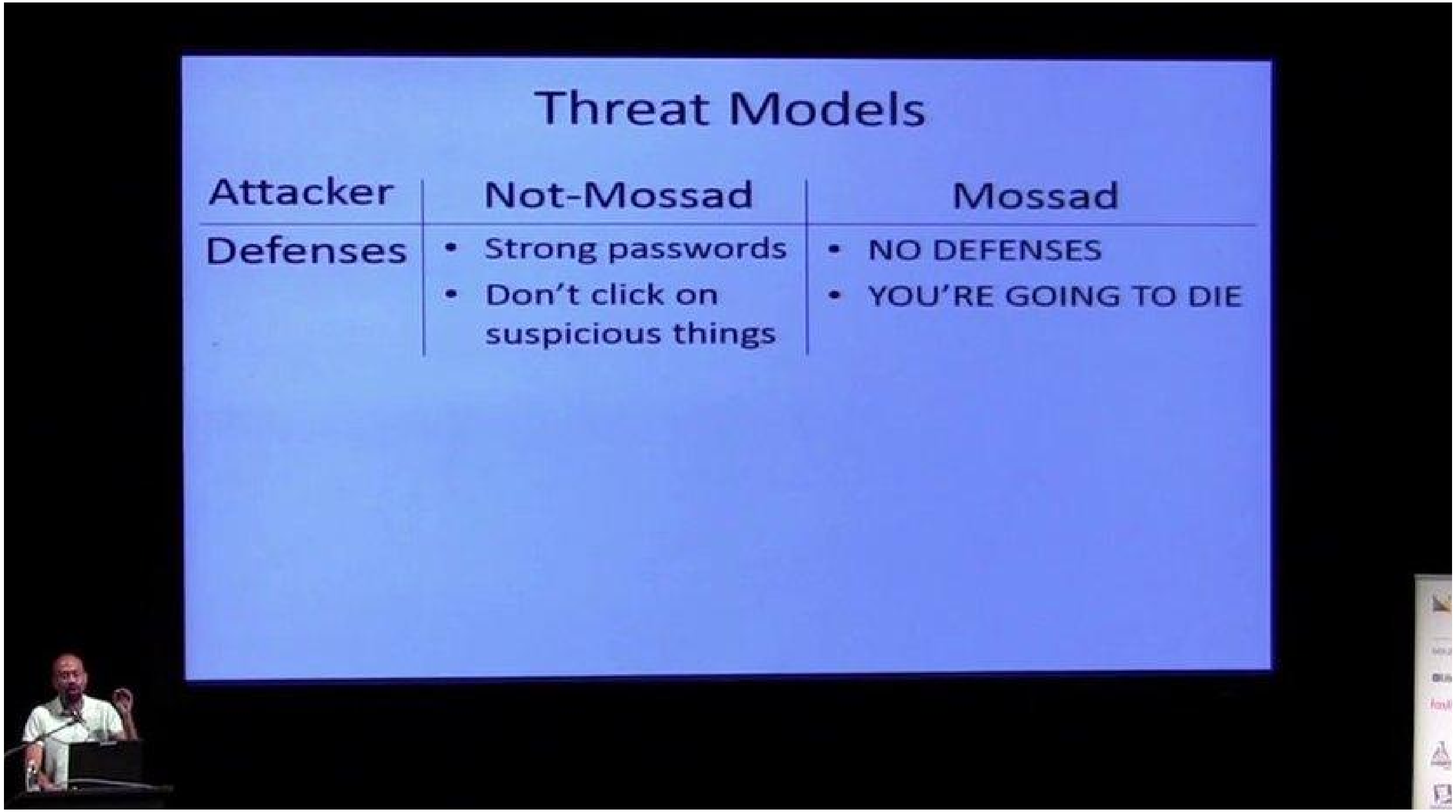
Dragnet vs Targeted—2/2

- They wouldn't bother trying to crack your crypto.
  - Assuming they can't already, that is…
    - (Attacks on RSA are getting worrying)
- They'd just correlate traffic (timing attacks).
  - Subpoena the ISP for logs (see NZ TICSA)
  - Subpoena any VPN provider for logs
- They'd just compromise the endpoints.
  - Subpoena the website for logs
  - Especially easy if you're using Windows
  - But even if you're *not*…


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

https://xkcd.com/538/

Threat models—1/4

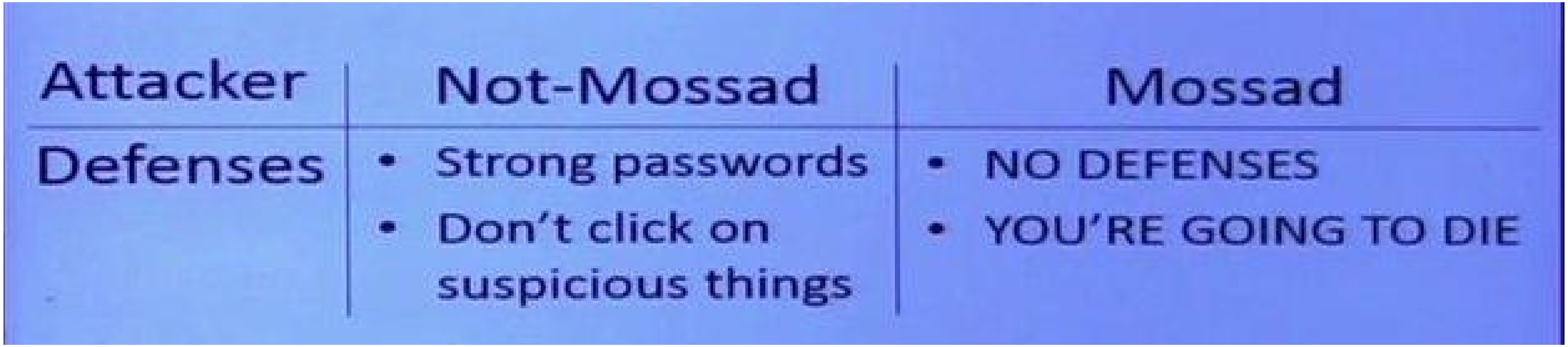


Threat Models

Attacker	Not-Mossad	Mossad
Defenses	• Strong passwords • Don’t click on suspicious things	• NO DEFENSES • YOU’RE GOING TO DIE

James Mickens at Monitorama

Threat models—2/4



Attacker	Not-Mossad	Mossad
Defenses	• Strong passwords • Don’t click on suspicious things	• NO DEFENSES • YOU’RE GOING TO DIE

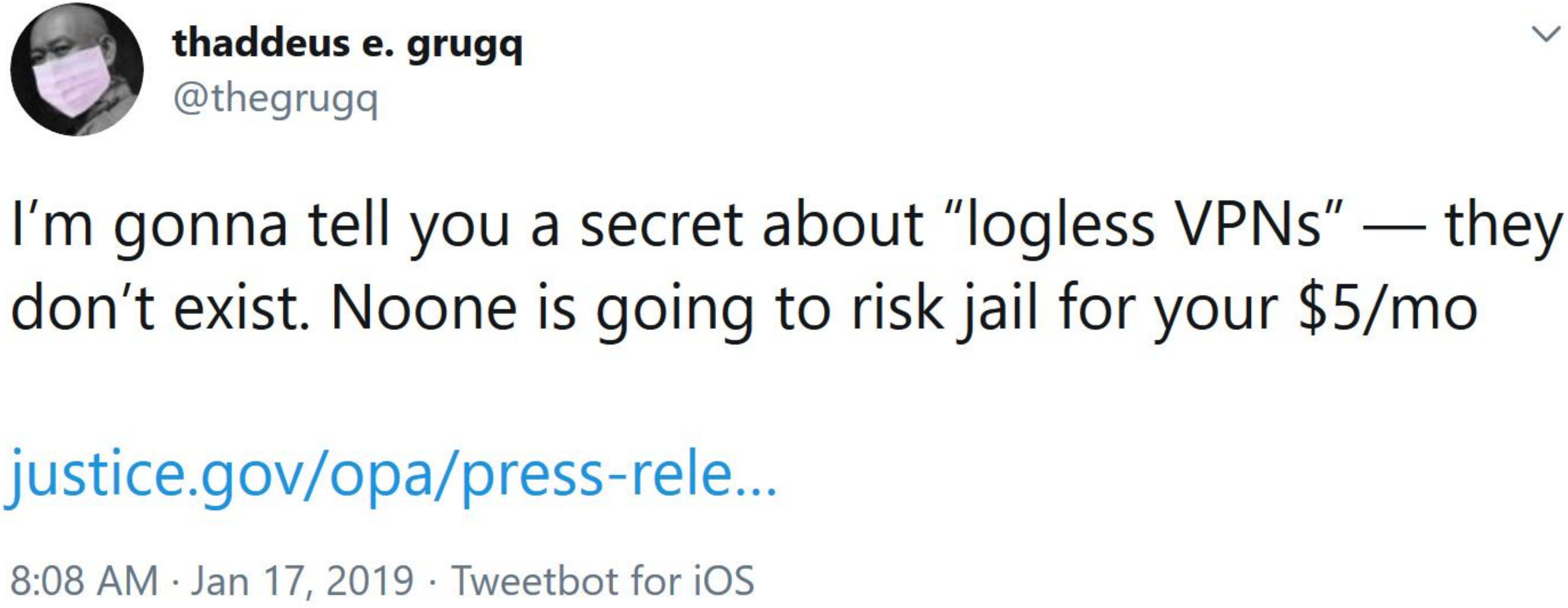
Threat models—3/4

- You *personally* are most likely not that interesting to nation-state surveillance.
  - And if you *are*, your PERSEC needs are *way* beyond my skill level…
- In fact, using Tor at all almost certainly makes you *more* interesting to nation-state actors.
  - Most security technologies do, after all.
  - Use PGP? You’re probably on a list somewhere.
  - Use a consumer proxy service like NordVPN? Yep…

Threat models—4/4

- The average person’s privacy needs are probably somewhat *simpler*…
  - *Browse* anonymously
  - *Create* anonymously (artists, minorities, those with socially-marginalised views…)
  - Bypass censorship
  - Hide your IP address
  - Hide your location
  - Avoid ads following you
  - Avoid marketing profiles
  - Avoid network logging, or smaller-scale surveillance (e.g. ISP)
  - Use hidden services

“What about my VPN?”—1/4



thaddeus e. grugq
@thegrugq

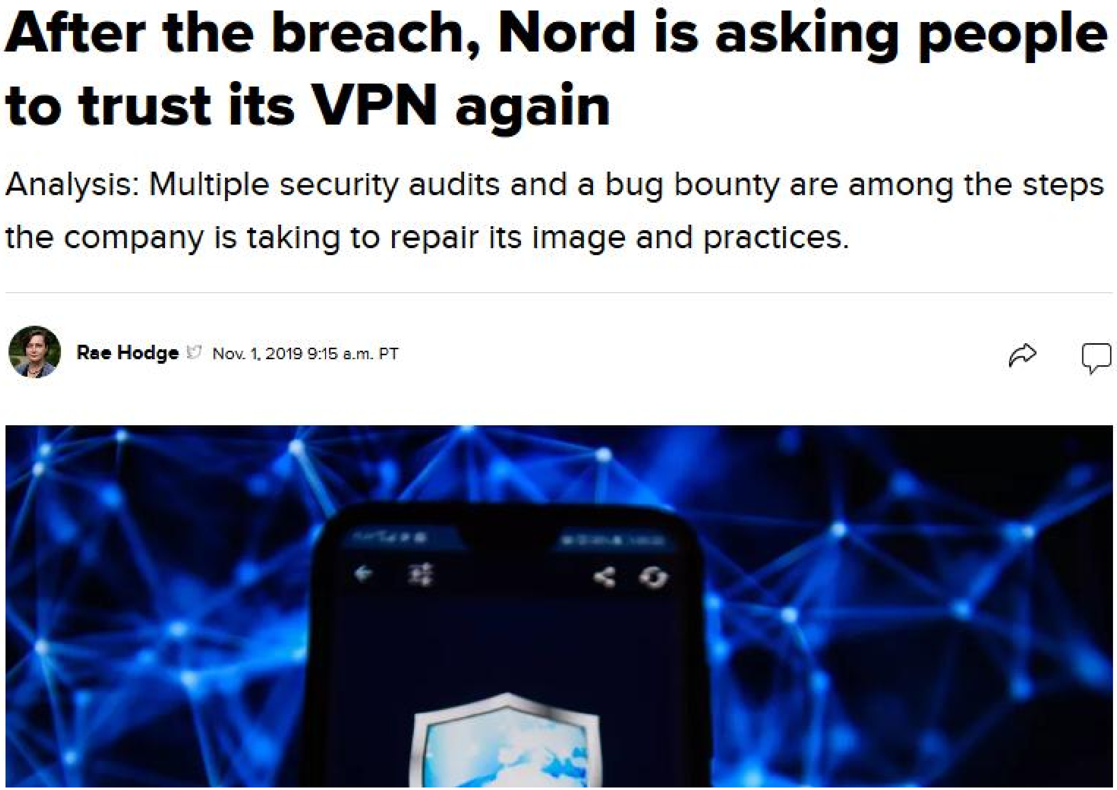
I’m gonna tell you a secret about “logless VPNs” — they don’t exist. Noone is going to risk jail for your $5/mo

justice.gov/opa/press-rele…

8:08 AM · Jan 17, 2019 · Tweetbot for iOS

https://twitter.com/thegrugq/status/1085614812581715968

“What about my VPN?”—2/4



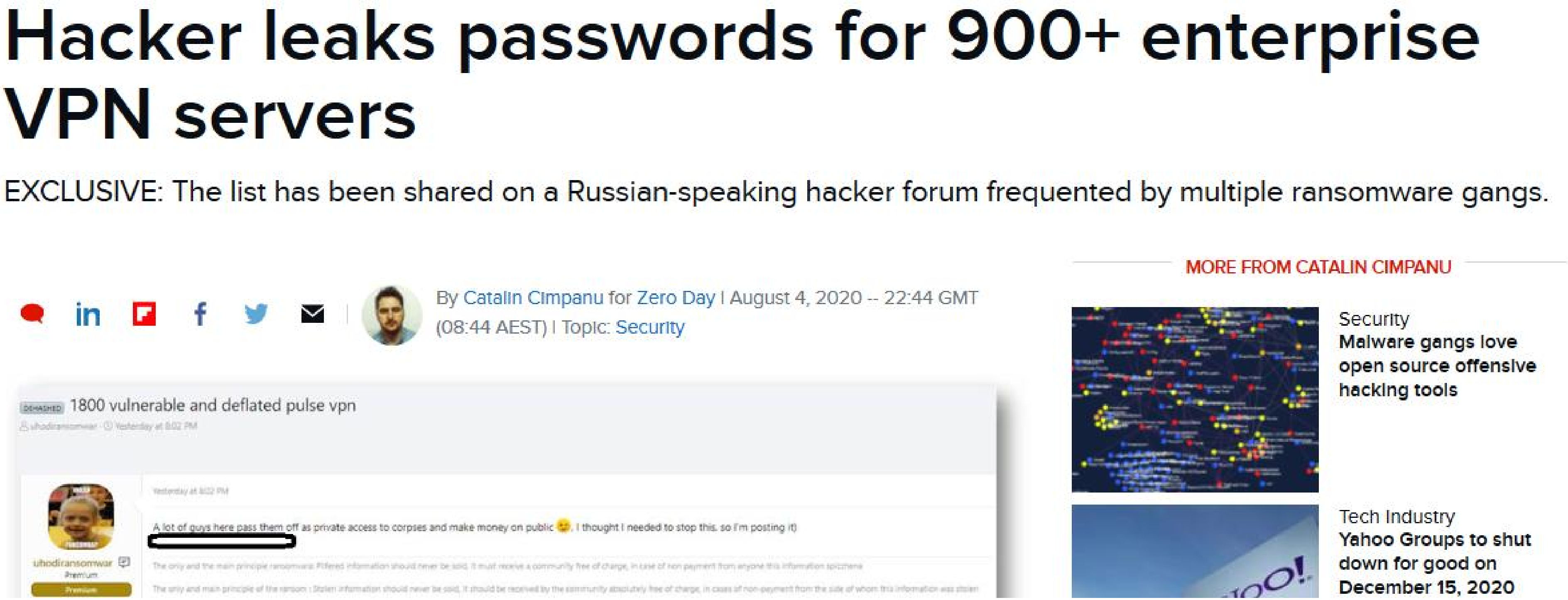
After the breach, Nord is asking people to trust its VPN again

Analysis: Multiple security audits and a bug bounty are among the steps the company is taking to repair its image and practices.

Rae Hodge Nov. 1, 2019 9:15 a.m. PT

https://www.cnet.com/news/after-the-breach-nord-is-asking-users-to-trust-it-again/

“What about my VPN?”—3/4



Hacker leaks passwords for 900+ enterprise VPN servers

EXCLUSIVE: The list has been shared on a Russian-speaking hacker forum frequented by multiple ransomware gangs.

By Catalin Cimpanu for Zero Day | August 4, 2020 -- 22:44 GMT (08:44 AEST) | Topic: Security

DEHASHED 1800 vulnerable and deflated pulse vpn

uhodiransomwar · Yesterday at 8:02 PM

uhodiransomwar
Premium
Premium

Yesterday at 8:02 PM

A lot of guys here pass them off as private access to corpses and make money on public 😉. I thought I needed to stop this. so I'm posting it)

[redacted]

The only and the main principle ransomware: Pilfered information should never be sold, it must receive a community free of charge, in case of non payment from anyone this information spizzhena

The only and main principle of the ransom : Stolen information should never be sold, it should be received by the community absolutely free of charge, in cases of non-payment from the side of whom this information was stolen

MORE FROM CATALIN CIMPANU

Security
Malware gangs love open source offensive hacking tools

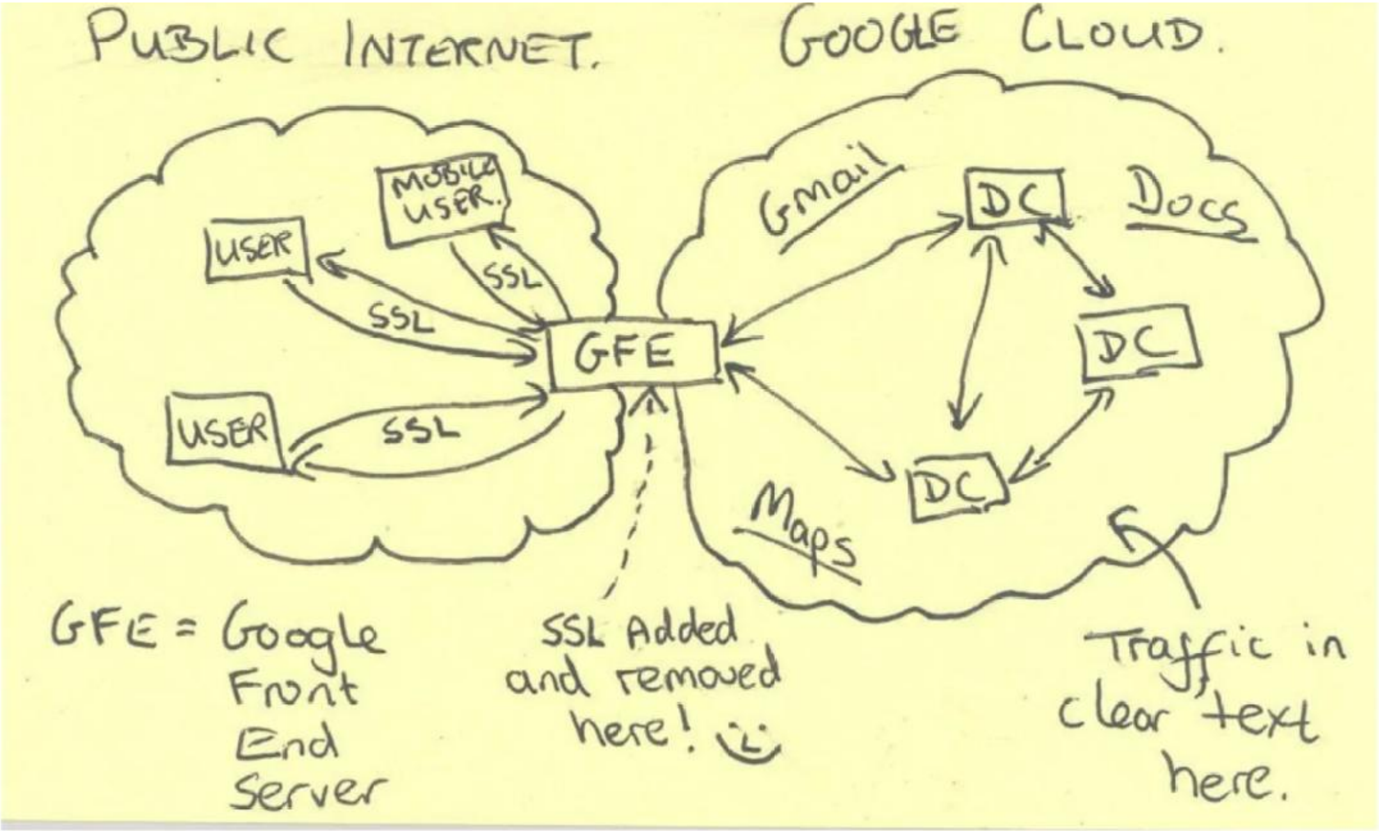
Tech Industry
Yahoo Groups to shut down for good on December 15, 2020

https://www.zdnet.com/article/hacker-leaks-passwords-for-900-enterprise-vpn-servers/

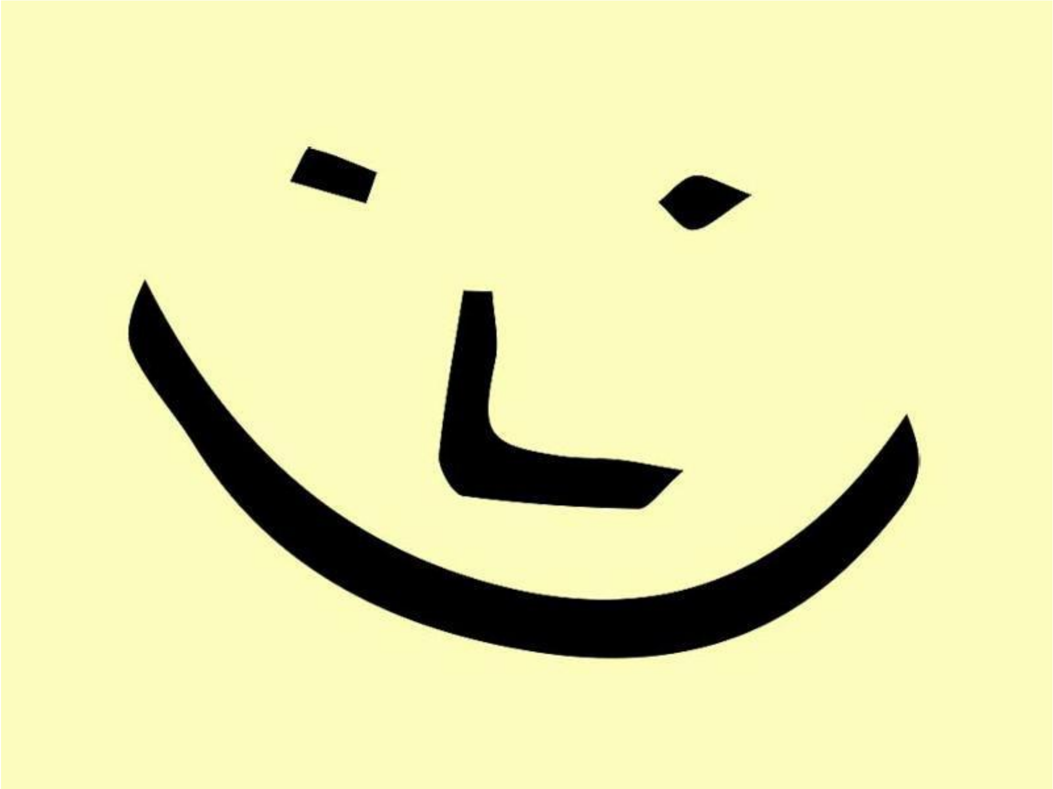
“What about my VPN?”—4/4

- The best way to keep information secret *isn’t* merely not to store it.
- It’s *never to have it in the first place*.
- Tor’s design is such that *only you* know both where the traffic is *from* and where it’s *going*.
- Traditional VPN providers can’t do that.

“What about SSL/TLS?”—1/3


PUBLIC INTERNET.
GOOGLE CLOUD.
MOBILE USER.
USER
USER
SSL
SSL
SSL
GFE
Gmail
DC
Docs
DC
DC
Maps
GFE = Google Front End Server
SSL Added and removed here! ☺
Traffic in clear text here.

“What about SSL/TLS?”—2/3



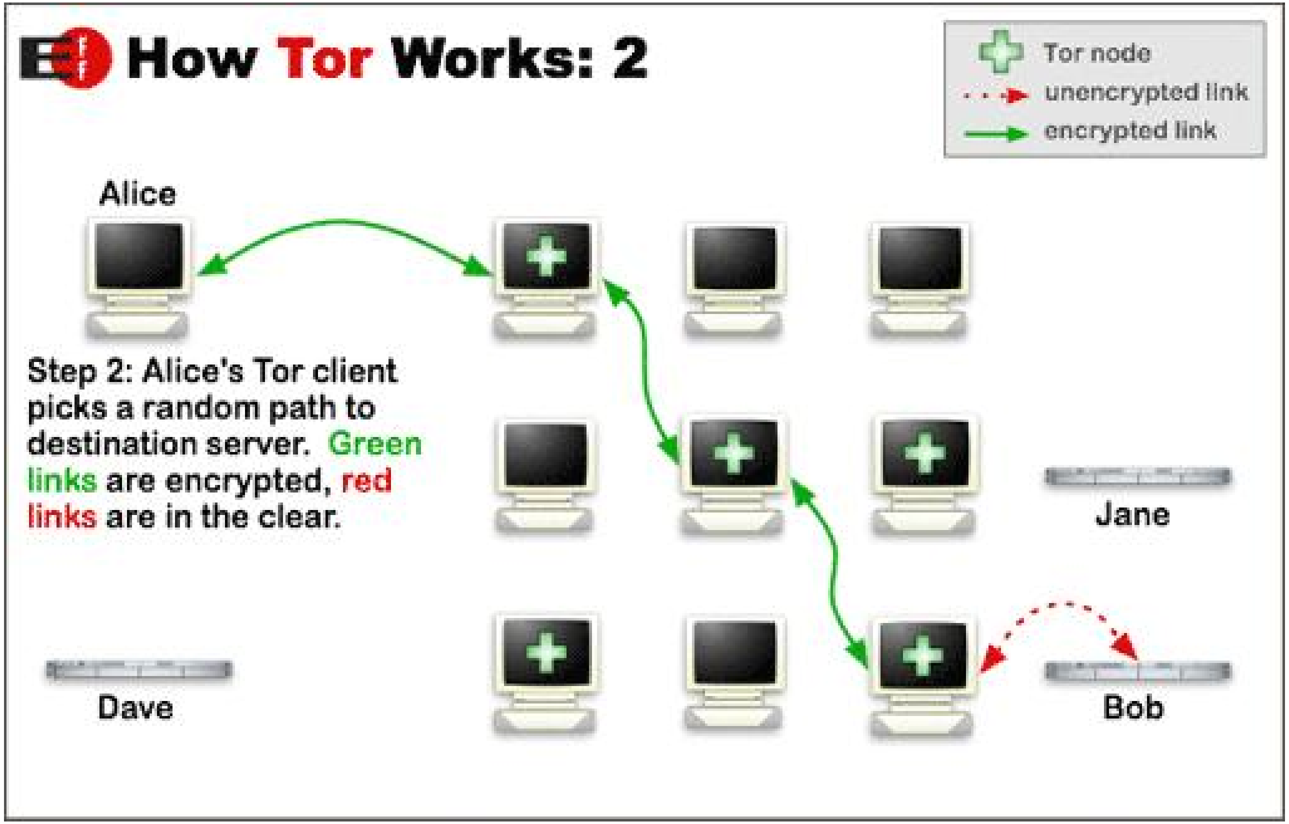
“What about SSL/TLS?”—3/3

- SSL/TLS (e.g. HTTPS) only encrypts your traffic between endpoints.
- Source and destination IPs and services are known to endpoints *and* transit nodes.
- If the remote end cooperates with or is compromised by surveillance, it won’t help you.

Onion routing—1/6

- Core principle: **Separate identification and routing.**
- Hosts in the network can route your traffic without having to know both its source and destination.
- This is done via **layers** of encryption…peeling off one layer at a time, like an onion.

Onion routing—2/6



Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.

https://2019.www.torproject.org/about/overview.html.en

Onion routing—3/6

1) **Your PC** chooses a **path** through the network.
2) It gets the **public keys** for each of the nodes it plans to send through.
3) It adds **three layers of encryption**—one for each node in the path.
4) It passes the data—the “**onion**”—to the first node.

Onion routing—4/6

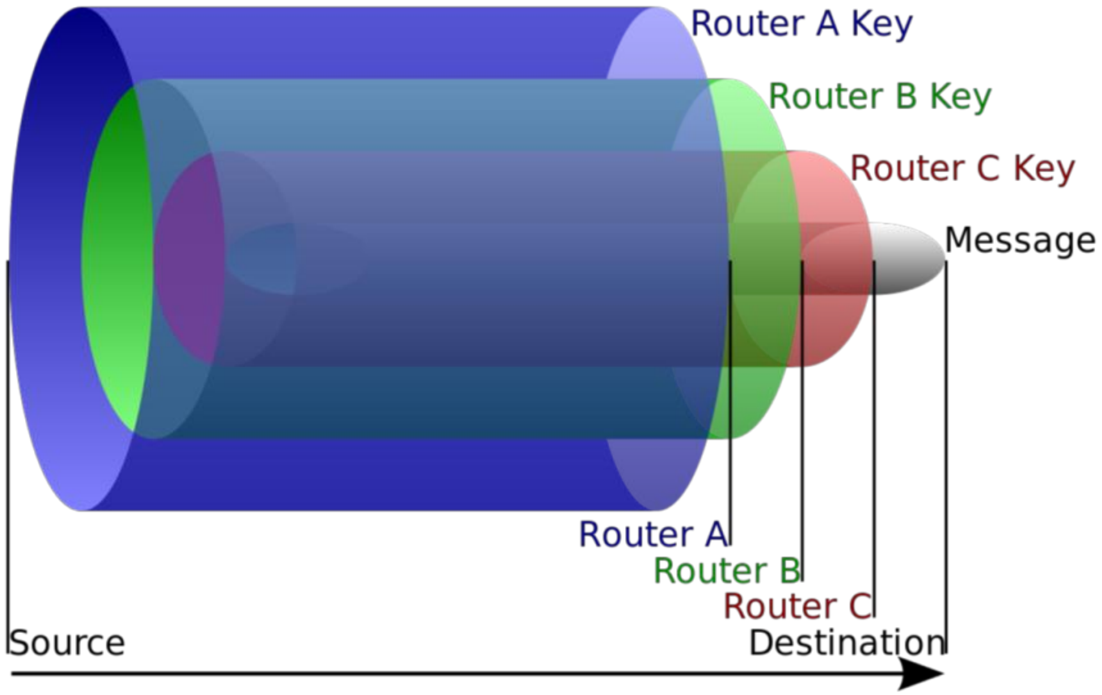


Image by Harrison Neal—https://commons.wikimedia.org/wiki/File:Onion_diagram.svg

Onion routing—5/6

- Nodes before the exit only know what the previous and next nodes are.
  - The first node doesn’t even know if your PC was the originator.
- Nodes before the exit cannot read the data themselves.
  - There are still layers to unwrap.

Onion routing—6/6

- For the response, the same path is followed *back*, with the same layered encryption applied, but in *reverse order*.
- All the nodes are *intentionally insulated* from data they don’t need.

Weaknesses—1/3

- **Protocols and user error:**
  - All the fancy routing in the world won’t help you if your protocol is designed to send out your IP address, timezone, hostname, language, CPU architecture…
    - Hint: **JavaScript**.
  - …or if you forget which browser you’re using, and try to log in to your Facebook account…
  - Tor is not magic security sauce.

Weaknesses—2/3

- **Timing attacks:**
  - If my ISP sees me get 123 KiB via Tor at 01:45:27 UTC…
  - …and a dodgy website my ISP hosts has logs showing a Tor request for 121 KiB bytes of `text/html`, gzip compressed, at 01:45:28 UTC…
- Do that a few thousand times, and my traffic can be *correlated*.

Weaknesses—3/3

- **Exit node compromise:**
  - Your exit nodes can read all your traffic after removing the encryption layers.
  - HTTPS and TLS in general are *even more* important on Tor—not less!
  - So is certificate verification!

Hidden services

- Hostnames end in `.onion`
- Might be hidden-only, might be available via clearnet too
- If hidden-only, neither you nor the site can identify one another
- Facebook (!!!) runs a surprisingly good one:

  https://facebookcorewwwi.onion/

  - It’s still Facebook, of course…use Tor Browser Bundle, and be careful what you tell them.

Demo—Tor Browser Bundle

Chat

- XMPP/Jabber works fine
- Some IRC networks let you connect via Tor:
  - freenode
  - OFTC
- This is particularly useful for IRC, which is otherwise a somewhat “leaky” protocol
- Hard to implement safely—gets abused by spammers
  - Current policy on freenode is to require at least *one* clearnet connection first
  - Shout-out to kline\0 and the other freenode staff for supporting this

BitTorrent

Please *don’t* use BitTorrent through Tor!

- Piracy seems to be the first application that most people think of
- BitTorrent protocol isn’t designed for privacy
- Harms the Tor network
- Slow
- Doesn’t work anyway (IP still disclosed)

Questions?

- Tor Project site:
  https://www.torproject.org/
- Onion routing:
  https://en.wikipedia.org/wiki/Onion_routing
- Threat models:
  https://en.wikipedia.org/wiki/Threat_model

Email: tom@sanctum.geek.nz

Website: https://sanctum.geek.nz/

Twitter: @tejrnz

Fediverse: @tejr@mastodon.sdf.org