IEEE: Social Implications of Technology

Andrew Lewman
andrew@torproject.org

March 19, 2012

Tor

TorProject.org
George Orwell
nineteen eighty-four
a novel
George Orwell was an optimist

“Who controls the past, controls the future: who controls the present controls the past”

— George Orwell, Nineteen Eighty Four, 1949
Internet Surveillance is getting more advanced

If You Can See It
You Can Monetize It

Evolved DPI – See what’s flowing through your network
Internet Surveillance is getting more advanced
'Comodo Hacker' Says He Acted Alone

The plot thickens: In an effort to back up his claims, alleged hacker dumps apparent evidence of pilfered database from breached Comodo reseller, as well as Mozilla add-on site certificate

By Kelly Jackson Higgins InformationWeek
April 09, 2011 12:00 AM

Comodo, a website certificate authority, revealed that nine SSL certificates were issued for fraudulent websites posing as domains for high-profile sites. Security researchers hope the incident will call attention to a certificate process they say is riddled with holes.
US company 'helped' Egypt block web

Egypt's crackdown on web users allegedly aided by US company's product.

Last Modified: 06 Feb 2011 03:23 GMT

When Egypt's uprising began nearly two weeks ago, there was a near-total internet blackout.

But exactly how was access cut off?

An American advocacy group called Free Press says it has uncovered a link to a California-based technology company that allegedly sold the Egyptian government equipment allowing it to track online activity.

Al Jazeera's Rob Reynolds reports.
Internet Surveillance is getting more advanced

China’s government is coming out with new measures to control the ability of citizens to acquire domains and setup personal sites, and to block hundreds of sites that offer illegal downloads of music, films, and video games.

In what appears to be another upgrade of the government’s already strict control of the Internet, Chinese authorities contest that the stricter controls are intended to protect children from pornography, limit piracy, and to make it hard to perpetuate Internet scams.

Under the new controls, more than 700 pornographic and
Exclusive: Top ISPs poised to adopt graduated response to piracy

by Greg Sandoval

Some of the country's largest Internet service providers are poised to leap into the antipiracy fight in a significant way.

After years of negotiations, a group of bandwidth providers that includes AT&T, Comcast, and Verizon are closer than ever to striking a deal with media and entertainment companies that would call for them to establish new and tougher punishments for customers who refuse to stop using their networks to pirate films, music and other intellectual property, multiple sources told CNET.

The sources cautioned that a final agreement has yet to be signed and that the partnership could still unravel but added that at this point a deal is within reach and is on track to be unveiled sometime next month.
Internet Surveillance is getting more advanced

[Diagram showing interconnected components of internet surveillance, including data exchange, ad exchange, ad server, buyers (advertisers and agencies), sellers (websites and ad networks), search engine optimization, retargeting, market researchers, affiliate marketers, and analytics services.]
Internet Surveillance is getting more advanced

**Combined Google Trackers**

Percentage of domains in data set with at least one Google web bug

(393,829 unique domains in set)

- **Google Analytics** (380,025) 71.2%
- **Google AdSense** (31,872) 35.5%
- **DoubleClick** (104,935) 26.6%
- **Google FriendConnect** (2,446) 0.6%
- **Google Widgets** (2,457) 0.6%

(348,059)
Internet Surveillance is getting more advanced
Internet Surveillance is getting more advanced

Click Here if you're paying more than $9.95 for phone!
Twitter in Iran: Good.

Iran Protests: Twitter, the Medium of the Movement
By LEV GROSSMAN  Wednesday, Jun. 17, 2009

Related Photos

Behind the Scenes with Mousavi

Stories
- In Iran, Rival Regime Factions Play a High-Stakes Game of Chicken
- Latest Tweets on Fallout from Iran's

Share

The U.S. State Department doesn't usually take an interest in the maintenance schedules of dotcom start-ups. But over the weekend, officials there reached out to Twitter and asked them to delay a network upgrade that was scheduled for Monday night. The reason? To protect the interests of

From http://www.time.com/time/world/article/0,8599,1905125,00.html
Twitter in USA: Bad.

FBI Raids Queens Home in G20 Protest Twitter Crackdown

That's right, a Twitter crackdown. A lawyer for Jackson Heights social worker Elliot Madison, 41, says that the feds searched his client's house for 16 hours on Thursday after Madison was arrested on September 24th at a Pittsburgh hotel room with another man. What were they up to? Sitting at laptops sending Twitter messages advising G20 demonstrators about riot police activity in the streets. And yet real Twitter threats like Lindsay Lohan and Courtney Love remain at large.

Madison, a self-described anarchist, was in Pittsburgh volunteering for the Tin Can Comms Collective, a group that uses Twitter to send mass text messages during protests describing events observed on the streets or over police scanners; stuff like "SWAT teams rolling down 5th Ave." Tin Can was active during the St. Paul RNC protests, and the authorities are now on to them. Madison was charged with hindering apprehension or prosecution, criminal use of a communication facility and possession of instruments of crime; he's currently out on bail.

from http://gothamist.com/2009/10/05/fbi_raids_queens_home_in_g20_protes.php
501(c)(3) non-profit organization dedicated to the research and development of technologies for online anonymity and privacy
What is Tor?

- online anonymity software and network
What is Tor?

- online anonymity software and network
- open source, freely available (3-clause BSD license)
What is Tor?

- online anonymity software and network
- open source, freely available (3-clause BSD license)
- active research environment:
  - Drexel, Univ of Waterloo, Georgia Tech, Princeton, Boston University, University College London, Univ of Minnesota, National Science Foundation, Naval Research Labs, Cambridge UK, Bamberg Germany, MIT...
What is Tor?

- online anonymity software and network
- open source, freely available (3-clause BSD license)
- active research environment:
  Drexel, Univ of Waterloo, Georgia Tech, Princeton, Boston University, University College London, Univ of Minnesota, National Science Foundation, Naval Research Labs, Cambridge UK, Bamberg Germany, MIT...
- increasingly diverse toolset:
  Tor, Tor Browser Bundle, Tails LiveCD, obfsproxy, Tor Weather, Tor auto-responder, Secure Updater, Orbot, Torora, Tor Check, Arm, Nymble, Tor Control, and so on.
Other Systems

- **VPN** - Virtual Private Network, 1 to 1 connection, can redirect all traffic, generally encrypted

- **Proxy** - 1 to 1 connection, per application traffic redirection, sometimes encrypted

- **I2P** - Garlic routing, closed network, anonymity and reputation

- **Freenet** - closed network, anonymity, distributed file storage and sharing

- **GNUnet** - closed network, anonymity, distributed file storage and sharing
Other Systems

- **VPN** - Virtual Private Network, 1 to 1 connection, can redirect all traffic, generally encrypted
- **Proxy** - 1 to 1 connection, per application traffic redirection, sometimes encrypted

I2P - Garlic routing, closed network, anonymity and reputation
Freenet - closed network, anonymity, distributed file storage and sharing
GNUnet - closed network, anonymity, distributed file storage and sharing
Other Systems

- **VPN** - Virtual Private Network, 1 to 1 connection, can redirect all traffic, generally encrypted
- **Proxy** - 1 to 1 connection, per application traffic redirection, sometimes encrypted
- **I2P** - Garlic routing, closed network, anonymity and reputation
- **Freenet** - closed network, anonymity, distributed file storage and sharing
- **GNUnet** - closed network, anonymity, distributed file storage and sharing
Other Systems

- **VPN** - Virtual Private Network, 1 to 1 connection, can redirect all traffic, generally encrypted
- **Proxy** - 1 to 1 connection, per application traffic redirection, sometimes encrypted
- **I2P** - Garlic routing, closed network, anonymity and reputation
- **Freenet** - closed network, anonymity, distributed file storage and sharing
Other Systems

- **VPN** - Virtual Private Network, 1 to 1 connection, can redirect all traffic, generally encrypted
- **Proxy** - 1 to 1 connection, per application traffic redirection, sometimes encrypted
- **I2P** - Garlic routing, closed network, anonymity and reputation
- **Freenet** - closed network, anonymity, distributed file storage and sharing
- **GNUnet** - closed network, anonymity, distributed file storage and sharing
How is Tor different from other systems?
How is Tor different from other systems?
How is Tor different from other systems?
Who uses Tor?

- Normal people
- Law Enforcement
- Human Rights Activists
- Business Execs
- Militaries
- Abuse Victims
Who uses Tor?

- **Normal users**
  linking sensitive information to their current identities, online advertising networks, search engines, censorship circumvention
Who uses Tor?

- Law enforcement
  accidental disclosure to targets, family and friend concerns, separating work from home life
Who uses Tor?

- **Rights Activists**
  Personal safety, family safety, narrowly-defined publicity, censorship circumvention
Who uses Tor?

- **Business Execs**
  - separating work from home life, competitor research, censorship circumvention
Who uses Tor?

- Abuse Victims and Survivors
  complete separation of past abuse and current life, finding help and safety, need to help others anonymously
Who uses Tor?

- **Normal users**
  - linking sensitive information to their current identities, online advertising networks, search engines, censorship circumvention

- **Law enforcement**
  - accidental disclosure to targets, family and friend concerns, separating work from home life

- **Rights Activists**
  - personal safety, family safety, narrowly-defined publicity, censorship circumvention

- **Business Execs**
  - separating work from home life, competitor research, censorship circumvention

- **Abuse Victims and Survivors**
  - complete separation of past abuse and current life, finding help and safety, need to help others anonymously

- **Militaries**
  - intelligence gathering, separating work from home life, other activities
Online and Offline change happens
You missed a use case

Security Blocks per category

- Botnet: 79.59%
- Malicious URLs: 14.32%
- Antivirus: 3.40%
- WRI: 0.02%
- Browser exploits: 0.10%
- Anonymizers: 0.02%
- Cookie stealing: 1.07%
- Phishing: 0.20%
- Adware/Spyware: 0.07%
- XSS: 1.21%
You missed a use case
You missed a use case

Help keep our classified business secret.
Don't discuss classified information out of the HQ.

Your Unit Supervisor is:  AGELA  (☎ 091 350 43 89)
You missed a use case
estimated 400k to 800k daily users
Tor hides communication patterns by relaying data through volunteer servers.
Tor hides communication patterns by relaying data through volunteer servers.
Tor hides communication patterns by relaying data through volunteer servers.
Tor hides communication patterns by relaying data through volunteer servers

Diagram: Robert Watson
Metrics

- Measuring metrics anonymously
- NSF research grant
- Archive of hourly consensus, ExoneraTor, VisiTor
- Metrics portal: https://metrics.torproject.org/
The text of this version is primarily taken from the first collected 1788 "McLean edition", but spelling and punctuation errors -- mainly printer's lapses -- have been corrected. The main heads have also been taken from that edition and are something like "The Same Subject Continued" we have repeated the previous heading and appended "(continued)", so have been guided by the excellent edition by Jacob E. Cooke, Wesleyan University Press, 1961. The footnotes are therefore used a variety of special typographical symbols for superscripts, we use numerals. Editors's footnotes are in original typography used for emphasis, such as all caps or italics, has been used here. We have tried to identify the newspapers were the Independent Journal [J], the New-York Packet [P], and the Daily Advertiser [A], all based in New York, actually first appeared May 28, 1788, in a bound volume published by J. and A. McLean, Federalist II. We have followed each paper to its primary author, James Madison [M], John Jay [J], or Alexander Hamilton [H], which is shown following.
dot onion you say?

http://duskgytldkxiuqc6.onion/fedpapers/federa00.htm
Thanks!

Visit https://www.torproject.org/ for more information, links, and ideas.
Credits & Thanks

- applied theory, fourth image: Al Jazeera, February 2011
- spring is in the air, Paco Pomet, http://pacopomet.wordpress.com/
- who uses tor?
  http://www.flickr.com/photos/mattw/2336507468/sizes/o/, Matt Westervelt, CC-BY-SA.
- danger!, http://flickr.com/photos/hmvh/58185411/sizes/o/, hmvh, CC-BY-SA.