SECURE Poland 2013

Andrew Lewman
andrew@torproject.org

09 October 2013

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

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Protocol</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.541</td>
<td>SYN from client to server</td>
<td>TCP</td>
<td>50936</td>
</tr>
<tr>
<td>0.541</td>
<td>ACK from server to client</td>
<td>TCP</td>
<td>50936</td>
</tr>
<tr>
<td>0.542</td>
<td>Client Hello</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.030</td>
<td>ACK from client to server</td>
<td>TCP</td>
<td>50936</td>
</tr>
<tr>
<td>1.033</td>
<td>Server Hello</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.124</td>
<td>ACK from server to client</td>
<td>TCP</td>
<td>50936</td>
</tr>
<tr>
<td>2.079</td>
<td>TCP Previous segment</td>
<td>TCP</td>
<td>50936</td>
</tr>
<tr>
<td>2.079</td>
<td>TCP Dup ACK 12#1</td>
<td>TCP</td>
<td>50936</td>
</tr>
<tr>
<td>5.563</td>
<td>TCP Retransmission</td>
<td>TCP</td>
<td>50936</td>
</tr>
<tr>
<td>5.563</td>
<td>ACK from client to server</td>
<td>TCP</td>
<td>50936</td>
</tr>
<tr>
<td>6.008</td>
<td>TCP Retransmission</td>
<td>TCP</td>
<td>50936</td>
</tr>
<tr>
<td>6.008</td>
<td>ACK from server to client</td>
<td>TCP</td>
<td>50936</td>
</tr>
<tr>
<td>16.025</td>
<td>Client Key Exchange</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17.533</td>
<td>TCP Retransmission</td>
<td>TCP</td>
<td>50936</td>
</tr>
<tr>
<td>20.735</td>
<td>TCP Retransmission</td>
<td>TCP</td>
<td>50936</td>
</tr>
<tr>
<td>21.127</td>
<td>TCP Previous segment</td>
<td>TCP</td>
<td>50936</td>
</tr>
<tr>
<td>26.447</td>
<td>FIN from client to server</td>
<td>TCP</td>
<td>50936</td>
</tr>
<tr>
<td>26.743</td>
<td>Encrypted Alert</td>
<td></td>
<td></td>
</tr>
<tr>
<td>26.743</td>
<td>ACK from server to client</td>
<td>TCP</td>
<td>50936</td>
</tr>
</tbody>
</table>
'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.
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 anti-Communist websites have been blocked.
Internet Surveillance is getting more advanced

Major ISPs agree to "six strikes" copyright enforcement plan

By Nate Anderson | Published 9 months ago

American Internet users, get ready for three strikes "six strikes." Major US Internet providers—including AT&T, Verizon, Comcast, Cablevision, and Time Warner Cable—have just signed on to a voluntary agreement with the movie and music businesses to crack down on online copyright infringers. But they will protect subscriber privacy and they won't filter or monitor their own networks for infringement. And after the sixth "strike," you
Internet Surveillance is getting more advanced
Internet Surveillance is getting more advanced

<table>
<thead>
<tr>
<th>Tracker</th>
<th>Number of unique domains found on</th>
<th>Percent of all unique domains</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Analytics</td>
<td>329,330</td>
<td>84%</td>
</tr>
<tr>
<td>Google Adsense</td>
<td>162,584</td>
<td>41%</td>
</tr>
<tr>
<td>DoubleClick</td>
<td>122,483</td>
<td>31%</td>
</tr>
<tr>
<td>Statcounter</td>
<td>26,806</td>
<td>7%</td>
</tr>
<tr>
<td>AddThis</td>
<td>24,126</td>
<td>6%</td>
</tr>
<tr>
<td>Quantcast</td>
<td>24,113</td>
<td>6%</td>
</tr>
<tr>
<td>Google Custom Search Engine</td>
<td>20,601</td>
<td>5%</td>
</tr>
<tr>
<td>OpenAds</td>
<td>17,608</td>
<td>4%</td>
</tr>
<tr>
<td>Omniture</td>
<td>13,126</td>
<td>3%</td>
</tr>
<tr>
<td>Wordpress Stats</td>
<td>11,475</td>
<td>3%</td>
</tr>
</tbody>
</table>

Figure 11 Percentage of Domains each Web bug was found on, March 2009
Internet Surveillance is getting more advanced

Click Here if you’re paying more than $9.95 for phone!

The new MacBook Pro
State-of-the-art processors. All-new graphics. Breakthrough high-speed I/O. Three very big leaps forward.
Internet Surveillance is getting more advanced
Internet Surveillance is getting more advanced
Internet Surveillance is getting more advanced

Tor Stinks... (u)

• We will never be able to de-anonymize all Tor users all the time.
• With manual analysis we can de-anonymize a very small fraction of Tor users, however, no success de-anonymizing a user in response to a TOPI request/on demand.
Twitter in Iran: Good.

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

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

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, NORDUnet...
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, NORDUnet...
- increasingly diverse toolset:
  Tor, Tor Browser Bundle, Tails LiveCD, Pluggable Transports, Tor Weather, Tor auto-responder, Secure Updater, Orbot, Gibberbot, Arm and so on.
FIRST RULE OF PRIVACY

I am the only one who can decide what I want to share.
Why Tor?

A HELPFUL VENN DIAGRAM
Who uses Tor?

- Normal people
- Law Enforcement
- Human Rights Activists
- Business Execs
- Militaries
- Abuse Victims
Online and Offline change happens
You missed a use case

THIS HIDDEN SITE HAS BEEN SEIZED

by the Federal Bureau of Investigation,
in conjunction with the IRS Criminal Investigation Division,
ICE Homeland Security Investigations, and the Drug Enforcement Administration,
in accordance with a seizure warrant obtained by the
United States Attorney’s Office for the Southern District of New York
and issued pursuant to 18 U.S.C. § 983(j) by the
United States District Court for the Southern District of New York
You missed a use case
You missed a use case
estimated 1 million daily users
How is Tor different from other systems?
How is Tor different from other systems?
How is Tor different from other systems?
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
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 the edition 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 follows.

The Federalist
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/
- danger!, http://flickr.com/photos/hmvh/58185411/sizes/o/, hmvh, CC-BY-SA.