Exclusively Relying on Tor Risks Detection and Exposure for Whistleblowers

By:

Michael Best

Tor Is A Tool, Not A Solution

- When creating a secure whistleblower platform:
  - The whistleblowers/end-users must be properly educated
  - **Multiple** toolsets must be employed
  - The inherent risks must be understood by ALL parties
  - The solutions must be adaptable to specific users and situations
    - **One size fits all is NOT an option!**

Inherent risks of Tor:

- Tor traffic **can** be identified
- Tor users **can** be de-anonymized
- Tor servers **can** be located
- Tor **can** be intercepted
- Tor traffic **can** be decrypted
- Tor **can** be used to infect it's users computers

Tor's Greatest Weakness

- Tor's greatest weakness is inseparable from its greatest strength: the unknown and ever-changing architecture of the system infrastructure.
- Relying on unknown parties creates opportunities to compromise Tor-based systems, or the whistleblowers relying on it.

Tor traffic

- Tor is designed to encrypt data and disguise it as normal HTTPS traffic
- **However**, Tor traffic can be identified by using a statistical analysis of the communication protocol in order to tell different SSL implementations apart
    - This can be performed by Off The Shelf software such as CapLoader

Identifying Tor traffic

- Tools like CapLoader can be deployed on Local or Wide Area Networks, by ISPs or anyone using legal or illegal wiretaps
    - ISPs are able to identify Tor traffic as part of their Standard Operating Procedure
- Once identified, the Tor traffic can be:
    - Blocked
    - Intercepted
    - Traced
    - Altered

De-anonymizing Tor Users

- Tor users can be easily located by monitoring networks for entry/access nodes to the Tor network
- 80% of all types of Tor users can be de-anonymized
    - Number increases to 95-100% if they are in common areas
    - Time to de-anonymize users decreases by orders of magnitude when resources exceed the absolute minimum technical requirements

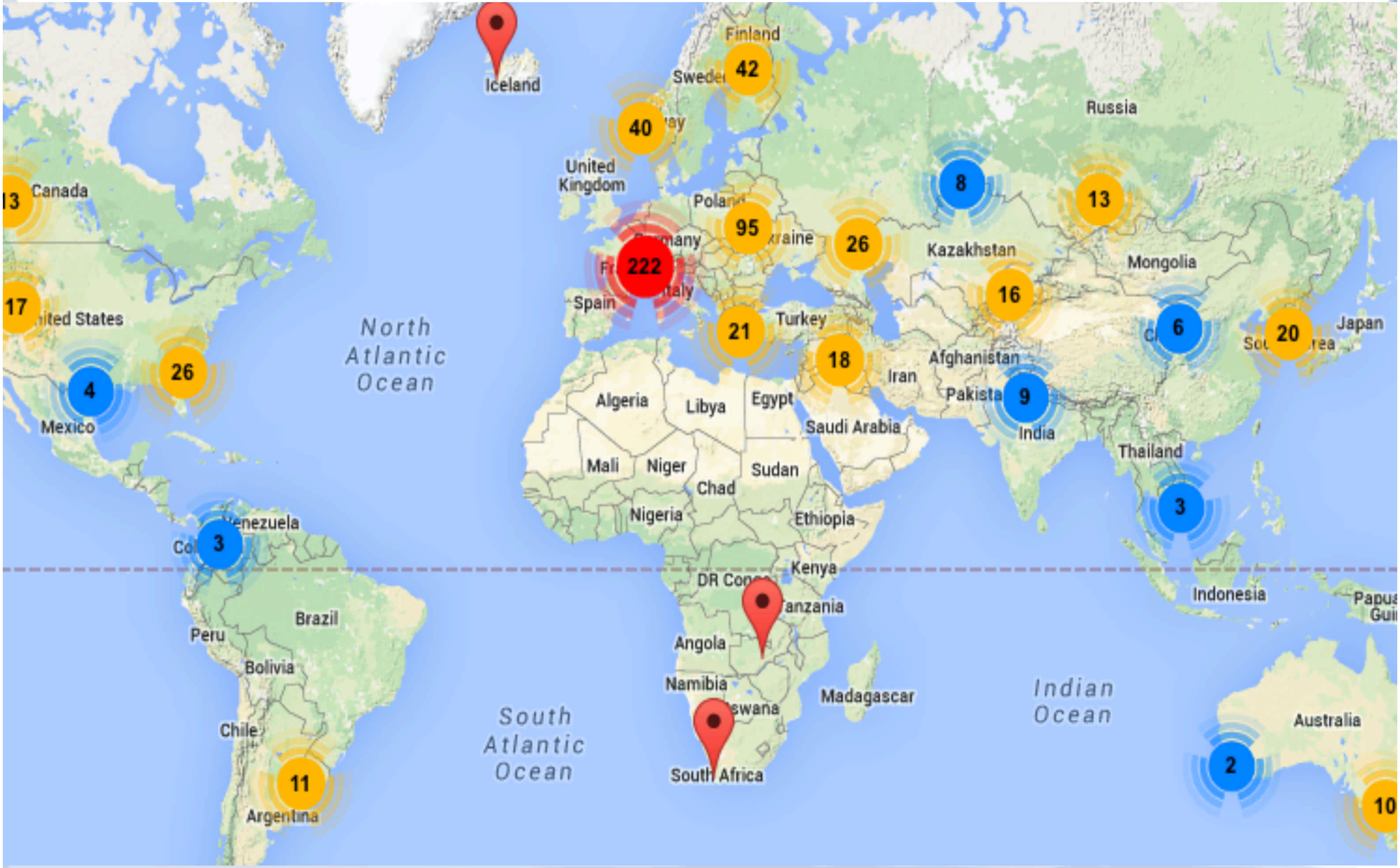
De-anonymizing events

- According to the Tor project, an attack de-anonymizing Tor users was detected in July 2014.
- The attacks specifically targeted people who operate or access Tor hidden services.
- According to the Tor project, “users who operated or accessed hidden services from early February through July 4 should assume they were affected.”
- This attack will **not** be the last of its kind.

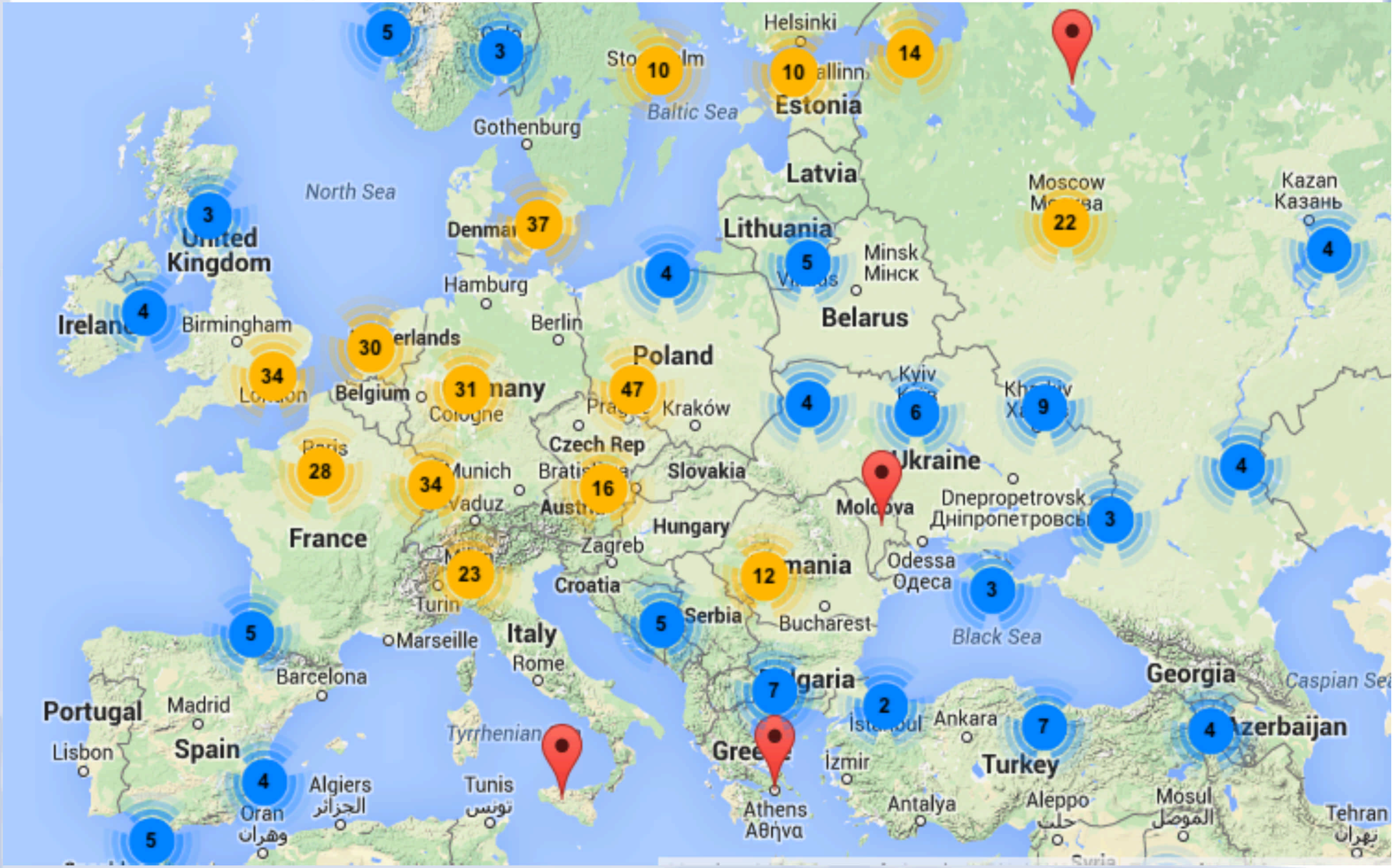
Locating Tor “Hidden” Servers

- Long-running hidden services using Tor can be identified more than 90% of the time
- Once the actual IP address is revealed, finding the server's physical location becomes a simple task
- Once located, it becomes simple to closely monitor the Tor server and those using it

Global Tor "Hidden" Servers



European Tor "Hidden" Servers



Once located...

- Physical access is total access
- The server/data can be stolen, destroyed, or even altered
- Data decrypted only on an air gapped computer is STILL vulnerable to:
    - Remote keyboard monitoring
    - Remote viewing/ computer monitor

Intercepting Tor

- Once the IP address of either the server or the individual is known, it is possible to:
  - Collect and copy the traffic
  - Block the traffic
- Hidden services are immune to exit node attacks, but still vulnerable to:
  - Malware
  - Brute force cracking

Cloning Tor Servers

- According to the Tor Project, vulnerabilities like Heartbleed can allow an attacker to impersonate a Tor hidden service
- This allows attackers to intercept all data and to prevent it from reaching the authentic server
    - No one be aware it was happening

Decrypting Tor

- Known vulnerabilities have already left Tor users vulnerable for months on end
- This will not be the last time Tor and other systems are compromised by a bug or by malware
    - There are an unknown number of Zero Day exploits yet to be discovered

Modifying Files Sent Through Tor

- Tor nodes have been detected modifying downloaded files with malware, compromising the system of users relying on the node
- .PDF and .DOC files can also be modified to compromise the recipient's system
- As previously mentioned, this can even **compromise air-gaped computers**

Addressing The Problem

- Provide additional drop systems with various non-Tor proxies
  - Explain the pros **and** cons of Tor and **other** proxies to your users
- **Whistleblowers should encapsulate Tor traffic in at least one additional layer of encryption and one additional proxy/relay**
- Understand that addressing the problem means thinking not in terms of security, but in terms of insecurity

Acknowledgements

- Defense Advanced Research Projects Agency
- U.S. Naval Research Laboratory
- Space and Naval Warfare Systems Center Pacific
- Georgetown University
- University of Cambridge
- Ben-Gurion University
- University of Luxembourg
- IEEE Symposium on Security and Privacy
- Tor Project
- Leviathan Security Group
- Offensive Security