Tor Mail

Tor Mail was a Tor hidden service that went offline in August 2013 after an FBI raid on Freedom Hosting. The service allowed users to send and receive email anonymously to email addresses inside and outside the Tor network.

History

Tor Mail provided web mail access with two webmail applications to choose from, one fully functional ajax-based, and one simple client which required no JavaScript or cookies. The user could also access mail via SMTP, POP3 or IMAP with an email client. The user signed up and accessed Tor Mail via the Tor hidden service and needed to have Tor software installed on a computer to access Tor hidden services. Users were not required to provide any identifying information such as their name or address.

Tor Mail's goal was to provide completely anonymous and private communications to anyone who needed it.[1] The service providers said that they were anonymous and could not be forced to reveal anything about a Tor Mail user. They also said that the service did not cooperate with anyone attempting to identify or censor a Tor Mail user.

Tor Mail's service consisted of several servers, the hidden service, and an incoming and outgoing internet facing mail servers. The site's operators said that the only data stored on the hard drive of those servers was the Exim mail server and the Tor software. "No emails, logs or personal data were stored on those servers, thus it doesn't matter if they are seized or shut down." They claimed to be prepared to quickly replace any relay that was taken offline. The service and SMTP/IMAP/POP3 were on a hidden server completely separate from the relays. The relays did not know the IP address of the hidden service.

2013 JavaScript attack

A message appeared on the Tor Mail main page in early August 2013, saying "Down for Maintenance Sorry, This server is currently offline for maintenance. Please try again in a few hours." Since August 2013, the service has been unavailable. The disappearance of Tor Mail has been linked to the arrest on child pornography charges of the alleged operator of Freedom Hosting, which hosted a large number of .onion sites.[2] In September 2013, the FBI admitted in a court filing in Dublin that it had taken down Freedom Hosting.[3]

The following month, details emerged of a zero-day JavaScript attack affecting the Tor Browser Bundle based on Firefox ESR 17 if JavaScript was enabled, as it was by default. Later versions of the Tor Browser Bundle disabled JavaScript by default. This zero-day vulnerability was exploited during the takedown to send users' IP addresses and Windows computer names to an FBI-controlled server in Virginia.[3][4] In January 2014 it was confirmed that the FBI had access to Tor Mail servers.[5]

In January 2016, it was claimed that innocent TorMail users may also have been subject to hacking by the FBI.[6]

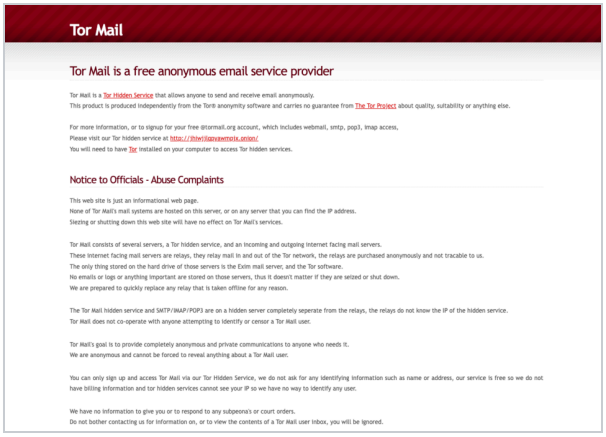
See also

- Anonymous remailer
- .onion domain
- Crypto-anarchism
- Internet privacy

References

1. "Notice to Officials - Abuse Complaints" (http://tormail.or/) .
2. "Freedom Hosting arrest and takedown linked to Tor privacy compromise" (https://nakedsecurity.sophos.com/2013/08/05/freedom-hosting-arrest-and-takedown-linked-to-tor-privacy-compromise/) . August 5, 2013. Archived (https://web.archive.org/web/20130810234834/http://nakedsecurity.sophos.com/2013/08/05/freedom-hosting-arrest-and-takedown-linked-to-tor-privacy-compromise/) from the original on August 10, 2013. Retrieved August 11, 2013.

Tor Mail



Screenshot of Tor Mail main page in April 2013

Type of site	Webmail
Available in	English
URL	tormail.org (https://web.archive.org/web/20121110101104/http://tormail.org/) Offline tormail.net (https://web.archive.org/web/20121026131112/http://www.tormail.net/) Offline
Commercial	No
Registration	Required
Users	unknown
Current status	Offline (as of 10 August 2013)

3. Poulsen, Kevin. "FBI Admits It Controlled Tor Servers Behind Mass Malware Attack" (https://www.wired.com/threatlevel/2013/09/freedom-hosting-fbi/) . *Wired*. Wired.com. Retrieved 2013-12-22.
4. "FBI Malware Analysis" (https://web.archive.org/web/20140417081750/http://ghowen.me/fbi-tor-malware-analysis/) . Gareth Owen. Archived from the original (http://ghowen.me/fbi-tor-malware-analysis) on 2014-04-17.
5. Poulsen, Kevin (2013-07-22). "If You Used This Secure Webmail Site, the FBI Has Your Inbox | Threat Level" (https://www.wired.com/threatlevel/2014/01/tormail/) . Wired.com. Archived (https://web.archive.org/web/20140128133914/http://www.wired.com/threatlevel/2014/01/tormail) from the original on 2014-01-28. Retrieved 2014-01-28.
6. Cox, Joseph (21 January 2016). "FBI May Have Hacked Innocent TorMail Users" (https://www.vice.com/en/article/fbi-may-have-hacked-innocent-tormail-users/) . Archived (https://web.archive.org/web/20160124030715/http://motherboard.vice.com/read/fbi-may-have-hacked-innocent-tormail-users) from the original on 24 January 2016. Retrieved 24 January 2016.