C24 A Freedom Hosting Darknet Case Study: Anatomy of a Takedown

Sarah Cortes, PhD, Inman Technology, 899 Green Street, San Francisco, CA 94133; and Gareth Owenson, PhD*, University of Portsmouth, University House, Winston Churchill Avenue, Portsmouth, HANTS PO1 2UP, UNITED KINGDOM*

After attending this presentation, attendees will better understand the step-by-step techniques by which the suspects in a famous darknet case were apprehended.

This presentation will impact the forensic science community by increasing awareness of the darknet, the capabilities of darknet tools, and the investigative techniques used in current cases. This presentation will detail results and conclusions as to effective techniques based on lab testing and increase awareness of criminal capabilities and how to counter them, as well as the legal issues that arise in these cases, and important implications for warrants and rules of evidence.

Using reverse engineering and other techniques, it will be demonstrated how security vulnerability exploits can help in investigating specific darknet cases. Additionally, this presentation will show how these techniques impact the forensic science community by increasing investigator capabilities and options in darknet cases, illustrated by their use in a major case — Freedom Hosting.

When the shutdown of online drug and contraband marketplaces AlphaBay and Hansa swept headlines in July 2017, United States Attorney General Jeff Sessions said: *"*... the forces of law and justice face a new challenge from the criminals and transnational criminal organizations who think they can commit their crimes with impunity by 'going dark.' "[1,2]

While the darknet has a number of legitimate uses, it has also become a haven for criminals.[3,4] Investigators have been developing, refining, and implementing techniques to infiltrate the darknet and use them to solve cases involving narcotics trafficking, carding, identity theft, child abuse, and other illegal activity which may be found there.[5-7] Here, one famous case, Freedom Hosting, is reviewed. This presentation will present a deep dive into technical options available and methods required to solve this, and other darknet cases, and to identify, apprehend, and arrest the suspect, Eric Eoin Marques.[8] A combination of techniques to de-anonymize darknet users will be shown.

Freedom Hosting was first targeted by the hacker collective calling itself "Anonymous" in what they called "Operation Darknet" around October 14, 2011.[9] Their attack targeted Lolita City and other child abuse websites on the darknet host Freedom Hosting. The attack, a vigilante operation, was not conducted by Law Enforcement Agencies (LEA). It disrupted but did not succeed in shutting down Freedom Hosting or its darknet websites. Its history helps illuminate the roots of later major darknet operations, including one referred to as Operation Freedom Hosting-2013, conducted by a collaboration of LEAs on the very same darknet host (Freedom Hosting) as Operation Darknet in 2011.

News of the 2013 operation came to light on August 1, 2013, when a reddit user mentioned in an obscure post that he had noticed some unusual "iframe" code on darknet internet service provider Freedom Hosting's websites.[10] On August 3, the local Dublin news service *Irish Independent* reported that Eric Eoin Marques, owner and administrator of Freedom Hosting, a website hosting company, had been arrested five days earlier in a classic phase A (website administrator) sting.[11,12] On August 4, 2013, Tor Project Executive Director Andrew Lewman confirmed to the world that a number of darknet sites had indeed disappeared from vendor platform Freedom Hosting.[13] On August 5, *Ars Technica* put together the local Dublin arrest story and the disappearing darknet sites, and the story went international.[13] We now know of this July 29, 2013, website host sting as a phase A of Operation Freedom Hosting.

What was also not publicly known for another year was that phase B of Operation Freedom Hosting was already underway. LEA deployed an investigative technique referred to as a Network Investigative Technique (NIT) for phase B on August 1-4, 2013. During this time, the Federal Bureau of Investigation (FBI) secretly controlled about 23 live Freedom Hosting sites, including some relatively innocuous sites, such as TorMail.[14,15] They displayed only an error message, while quietly deploying a NIT to catch users.[15] The sting had expanded to target not only the host's administrator, but also site users. In 2014, FBI and Department Of Justice (DOJ) warrants, complaints, and affidavits became public, confirming the operation. The press and public had been distracted with the report of Marques's arrest, not widely realizing that another, wider sting was already underway.

Documents indicate that a NIT had revealed the identities not only of child abuse site administrators, but also of site users. In phase B, the FBI seized and operated the 23 Freedom Hosting websites, deployed NITs, identified site users, and set in motion the arrest and prosecution of users. These users included David and Teri Schell, who were also Silk Road 2.0 sellers, and Grant Klein for child abuse offences.[16,17] While investigators have prevailed in this and many other darknet cases, it is sobering to note that as of February 2017, a darknet website calling itself Freedom Hosting still operates on the darknet.[18]

Reference(s):

1. Johnson, A, Jaggard, A, Cortes, S., Feigenbaum, J., Syverson, P. (2015) 20,000 In League Under the Sea: Anonymous Communication, Trust, MLATs, and Undersea Cables. In: *Proceedings on Privacy Enhancing Technologies, 9th International Symposium (PETS 2015).*

2. Owenson, G.H. and Savage, N.J. (2016). Empirical analysis of Tor hidden services. In: *IET Information Security.* 10, 3, p. 113-118, https://researchportal.port.ac.uk/portal/en/publications/empirical-analysis-of-tor-hidden-services(309104be-8c31-4498-9ed3-ab1be058ffe8).html.

3. Gareth Owenson. *Analysis of the FBI Tor Malware.* Dr Gareth Owenson's blog, Aug 8, 2013, http://blog.owenson.me/analysis-of-the-fbi-tor-malware.

4. Anonymous. *Operation Darknet.* YouTube (Oct. 17, 2011), https://www.youtube.com/watch?v=aFuJp_zPIlU.

Copyright 2018 by the AAFS. Permission to reprint, publish, or otherwise reproduce such material in any form other than photocopying must be obtained by the AAFS.

*Presenting Author

5. Founder of the Freedom Hosting arrested, held without bail in Ireland, awaiting extradition to the USA. Reddit (Aug. 1, 2013), https://www.reddit.com/r/onions/comments/1jmrta/founder_of_the_freedom_hosting_arrested_held (Op FH).
6. Brian Krebs, Firefox Zero-Day Used in Child Porn Hunt? *Krebs on Security.* August 4, 2013, https://krebsonsecurity.com/2013/08/firefox-zero-day-used-in-child-porn-hunt/#more-22123 (Op FH). See also Sharwood, Simon, Tor servers vanish as FBI swoops on kiddie-smut suspect. Reports say user IP addresses revealed, mail down, malware spreading. *The Register* (Aug. 5, 2013), http://www.theregister.co.uk/2013/08/05/tor_servers_vanish_as_fbi_swoops_on_kiddiesmut_suspect (Op FH).
7. McDonald, Dearbhail. Largest facilitator of child porn on planet must wait month for FBI case. *Irish Indepentent.* (Aug.3, 2013), http://www.independent.ie/irish-news/courts/largest-facilitator-of-child-porn-on-planet-must-wait-month-for-fbicase-29501879.html (Op FH).
8. http://dailycaller.com/2016/08/23/lawyers-fbi-was-largest-distributer-of-child-porn-on-the-darknet.
9. Irish Court of Appeal, Marques v. Director of Public Prosecutions & ors.
10. http://www.bailii.org/cgi-bin/format.cgi?doc=/ie/cases/IECA/2016/CA373.html&query=(eric)+AND+(eoin)+AND+(marques)#disp1.
11. Lewman, Andrew. *Hidden Services, Current Events, and Freedom Hosting.* Tor Blog (Aug. 4, 2013), https://blog.torproject.org/blog/hidden-services-current-events-and-freedom-hosting (Op FH). and available here: https://blog.lewman.is/2013/08/04/hidden-services-current-events-and-freedom-hosting.
12. Dan Gooding. Attackers wield Firefox exploit to uncloak anonymous Tor users. *Ars Technica.* (Aug. 5, 2013), http://arstechnica.com/security/2013/08/attackers-wield-firefox-exploit-to-uncloak-anonymous-tor-users (Op FH).
13. Ellen Nakashima. This is how the government is catching people who use child porn sites. *Washington Post.* (Jan. 21, 2016), https://www.washingtonpost.com/world/national-security/how-the-government-is-using-malware-to-ensnare-child-porn-users/2016/01/21/fb8ab5f8-bec0-11e5-83d4-42e3bceea902_story.html?postshare=6721453401674096&tid=ss_tw&utm_term=.dcb23b1710ff.
14. Joseph Cox. FBI May Have Hacked Innocent TorMail Users. *Motherboard.* (Jan 21, 2016), https://motherboard.vice.com/en_us/article/fbi-may-have-hacked-innocent-tormail-users.
15. Joseph Cox. Sorry Guys, The FBI Did Not Run 23 Child Porn Websites. *Medium*. (Nov. 12, 2016), https://medium.com/@josephfcox/sorry-guys-the-fbi-did-not-run-23-child-porn-websites-c0457424286b#.jm659omff (Op FH).
16. Kale Williams. Butte County couple ensnared in Silk Road 2.0 drug case. *San Francisco Chronicle*. (Nov. 21, 2014).
17. http://www.sfgate.com/crime/article/NorCal-couple-ensnared-in-dark-Web-drug-site-5907946.php (Op FH).
18. FBI Press Release. Brattleboro Man Sentenced to Prison for Child Pornography Offense.

Darknet, Tor, Freedom Hosting

Copyright 2018 by the AAFS. Permission to reprint, publish, or otherwise reproduce such material in any form other than photocopying must be obtained by the AAFS.