WHAT IF THE TOR TAKEDOWN RELATES TO THE YEMENI ALERT?

Eli Lake and Josh Rogin reveal that the intercept between Ayman al-Zawahiri and Nasir al-Wuhayshi was actually a conference call between those two and affiliates all over the region.

> The Daily Beast has learned that the discussion between the two al Qaeda leaders happened in a conference call that included the leaders or representatives of the top leadership of al Qaeda and its affiliates calling in from different locations, according to three U.S. officials familiar with the intelligence. All told, said one U.S. intelligence official, more than 20 al Qaeda operatives were on the call.
>
> To be sure, the CIA had been tracking the threat posed by Wuhayshi for months. An earlier communication between Zawahiri and Wuhayshi delivered through a courier was picked up last month, according to three U.S. intelligence officials. But the conference call provided a new sense of urgency for the U.S. government, the sources said.

The fact that al Qaeda would be able to have such conference calls in this day and age is stunning. The fact that US and Yemeni sources would expose that they knew about it is equally mind-boggling.

But one thing would make it make more sense.

On Sunday, Tor users first discovered the FBI had compromised a bunch of onion sites and introduced malware into FireFox browsers accessing the system. Since then, we’ve learned the malware was in place by Friday, the day the

US first announced this alert (though the exploit in FireFox has been known since June).

> The owner of an Irish company, Freedom Hosting, has allegedly been providing turnkey hosting services for the Darknet, or Deep Web, which is “hidden” and only accessible through Tor .onion and the Firefox browser. The FBI reportedly called Eric Eoin Marques “the largest facilitator of child porn on the planet” and wants to extradite the 28-year-old man. About that time, Freedom Hosting went down; Tor users discovered that someone had used a Firefox zero-day to deliver drive-by-downloads to anyone who accessed a site hosted by Freedom Hosting. Ofir David, of Israeli cybersecurity firm Cyberhat, told Krebs on Security, “**Whoever is running this exploit can match any Tor user to his true Internet address, and therefore track down the Tor user**.”
>
> If you’ve never visited the Hidden Wiki, then you should be fully aware that if you do, you *will* see things that can never be unseen. Freedom Hosting maintained servers for “TorMail, long considered the most secure anonymous email operation online,” wrote Daily Dot. “Major hacking and fraud forums such as HackBB; large money laundering operations; and the Hidden Wiki, which, until recently, was the de facto encyclopedia of the Dark Net; and virtually all of the most popular child pornography websites on the planet.”
>
> But if you use Tor Browser Bundle with Firefox 17, you accessed a Freedom Hosting hidden service site since August 2, and you have JavaScript enabled, then experts suggest it’s likely your machine has been compromised. In fact, E Hacking News claimed that almost half of all Tor sites have been compromised by the FBI.

> [my emphasis]

So what if this takedown was only secondarily about child porn, and primarily about disabling a system al Qaeda has used to carry out fairly brazen centralized communications? Once the malware was in place, the communications between al Qaeda would be useless in any case (and I could see the government doing that to undermine the current planning efforts).

The timing would all line up — and it would explain (though not excuse) why the government is boasting about compromising the communications. And it would explain why Keith Alexander gave this speech at BlackHat.

> terrorists … terrorism … terrorist attacks … counterterrorism … counterterrorism … terrorists … counterterrorism … terrorist organizations … terrorist activities … terrorist … terrorist activities … counterterrorism nexus … terrorist actor … terrorist? … terrorism … terrorist … terrorists … imminent terrorist attack … terrorist … terrorist-related actor … another terrorist … terrorist-related activities … terrorist activities … stopping terrorism … future terrorist attacks … terrorist plots … terrorist associations
>
> [snip]
>
> Sitting among you are people who mean us harm

Just one thing doesn't make sense.

Once NSA/FBI compromised Tor, they'd have a way to identify the location of users. That might explain the uptick in drone strikes in Yemen in the last 12 days. But why would you both alert Tor users and — with this leak — Al Qaeda that you had broken the system and could ID their location? Why not roll up the network first, and then take down the Irish child porn guy who is the likely target?

I’m not sure I understand the Tor exploit well enough to say, but the timing does line up remarkably well.

Update: Some re-evaluation of what really happened with the exploit.

> Researchers who claimed they found a link between the Internet addresses used as part of malware that attacked Freedom Hosting’s “hidden service” websites last week and the National Security Agency (NSA) have backed off substantially from their original assertions. After the findings were criticized by others who analyzed Domain Name System (DNS) and American Registry for Internet Numbers (ARIN) data associated with the addresses in question, Baneki Privacy Labs and Cryptocloud admitted that analysis of the ownership of the IP addresses was flawed. However, they believe the data that they used to make the connection between the address and the NSA may have changed between their first observation.

Update: On Twitter, Lake clarifies that this conference call was not telephone-based communications.