TAKEDOWNS OF SHADOW BROKERS FILES AFFIRM FILES AS STOLEN

I've been wondering something.

Almost immediately after the Shadow Brokers posted their Equation Group files, GitHub, Reddit, and Tumblr took down the postings of the actual files. In retrospect, it reminded me of the way Wikileaks was booted off PayPal in 2010 for, effectively, publishing files.

So I sent email to the three outlets asking on what basis they were taken down. GitHub offered the clearest reason. In refreshingly clear language, its official statement said,

> Per our Terms of Service (section A8), we do not allow the auction or sale of stolen property on GitHub. As such, we have removed the repository in question.

Mind you, A8 prohibits illegal purpose, not the auction of stolen property:

> You may not use the Service for any illegal or unauthorized purpose. You must not, in the use of the Service, violate any laws in your jurisdiction (including but not limited to copyright or trademark laws).

Moreover, at least in its Pastebin explanation, Shadow Brokers were ambiguous about how they obtained the files.

> How much you pay for enemies cyber weapons? Not malware you find in networks. Both sides, RAT + LP, full state sponsor tool set? *We find* cyber weapons made by creators of stuxnet, duqu, flame. Kaspersky calls Equation

> Group. We follow Equation Group traffic. *We find Equation Group source range. We hack Equation Group. We find many many Equation Group cyber weapons*. You see pictures. We give you some Equation Group files free, you see. This is good proof no? You enjoy!!! You break many things. You find many intrusions. You write many words. But not all, we are auction the best files.

They state they "found" the files, or at least traces of the files, and only say they "hacked" to obtain them to get to the latest stage. If they (in the Russian theory of the files) were "found" on someone's own system, does that count as "stealing" property?

Tumblr wasn't quite as clear as GitHub. They said,

> Tumblr is a global platform for creativity and self-expression, but we have drawn lines around a few narrowly defined but deeply important categories of content and behavior, as outlined in our Community Guidelines. The account in question was found to be in violation of these policies and was removed.

But it's not actually clear what part of their user guidelines Shadow Brokers violated. They've got a rule against illegal behavior.

> - ***Unlawful Uses or Content.*** *Don't use Tumblr to conduct illegal behavior, like fraud or phishing. That should be pretty obvious to you, a decent human being.*

I guess the sale of stolen property is itself illegal, but that goes back to the whole issue of Shadow Brokers' lack of clarity of how they got what they got. Their property specific guidelines require someone to file a notice.

> Intellectual property is a tricky issue, so now is as good a time as any to explain some aspects of the process we use for handling copyright and trademark complaints. We respond to notices of alleged copyright infringement as per our Terms of Service and the Digital Millennium Copyright Act; please see our DMCA notification form to file a copyright claim online. Please note that we require a valid DMCA notice before removing content. Parties asserting a trademark infringement claim should identify the allegedly infringing work and the legal basis for their claim, and include the registration and/or application number(s) pertaining to their trademark. Each claim is reviewed by a trained member of our Trust and Safety team.
>
> If we remove material in response to a copyright or trademark claim, the user who posted the allegedly infringing material will be provided with information from the complainant's notice (like identification of the rightsholder and the allegedly infringed work) so they can determine the basis of the claim.

The tech companies might claim copyright violations here (or perhaps CFAA violations?), but the files came down long before anyone had publicly IDed them as the victims. So the only "owner" here would be the NSA. Did they call Tumblr AKA Verizon AKA a close intelligence partner of the NSA?

Finally, Shadow Brokers might be in violation of Tumblr's unauthorized contests.

> - ***Unauthorized Contests, Sweepstakes, or Giveaways.*** *Please follow our guidelines for contests, sweepstakes, and giveaways.*

The guidelines say you can link to whackjob contest (which this is) elsewhere, but you do have to make certain disclosures on Tumblr itself.

One more thing about Tumblr, though. It claims it will give notice to a user before suspending their content.

Finally, there's Reddit, which blew off my request altogether. Why would they take down Shadow Brokers, given the range of toxic shit they permit to be posted?

They do prohibit illegal content, which they describe as,

> Content may violate the law if it includes, but is not limited to:
>
> - *copyright or trademark infringement*
> - *illegal sexual content*

Again, GitHub's explanation of this as selling stolen property might fit this description more closely than copyright infringement, at least of anyone who would have complained early enough to have gotten the files taken down.

The more interesting thing about Reddit is they claim they'll go through an escalating series of warning before taking down content, which pretty clearly did not happen here.

> We have a variety of ways of enforcing our rules, including, but not limited to

> - *Asking you nicely to knock it off*
> - *Asking you less nicely*
> - *Temporary or permanent suspension of accounts*
> - *Removal of privileges from, or adding restrictions to, accounts*
> - *Adding restrictions to Reddit communities, such as adding NSFW tags or Quarantining*
> - *Removal of content*
> - *Banning of Reddit communities*

Now, don't get me wrong. These are dangerous files, and I can understand why social media companies would want to close the barn door on the raging wild horses that once were in their stable.

But underlying it all appears to be a notion of property that I'm a bit troubled by. Even if Shadow Brokers stole these files from NSA servers — something not at all in evidence — they effectively stole NSA's own tools to break the law. But if these sites are treating the exploits themselves as stolen property, than so would be all the journalism writing about it.

Finally, there's the question of how these all came down so quickly. Almost as if someone called and reported their property stolen.