Blast Accusations for Cybersecurity Intel

By akerch

Cheating on your spouse is the perfect example of an ethical gray area. No, it's not technically illegal, but it's not exactly a good thing to do, and it is surely not something you'd want many people finding out about. Anybody cheating on their spouse, especially those who think nobody knows, would be scared by an email or letter accusing them of infidelity, and if that correspondence demanded money to keep the secret, some cheaters might just pay up. It's no surprise, then, that ransom-demanding, cheater-accusing blast letters are a recent trend in the blackmailing world.[1]

The world of cybersecurity, where individuals and their actions often exist in the gray area between legal and illegal, is no different: accusations of guilt can carry a lot of weight. If preying on secrets by choosing something that a small to moderate amount of people are probably guilty of and sending out a blast letter accusing everybody of that guilt can work to expose cheating spouses, could it be used for exposing cyber criminals? That is, if a cyber investigation group had a list of potential criminals and their email addresses, could sending out an email to every single one of them accusing them of a crime make the ones who are truly guilty come forward?

The potential effects of using this type of tactic to help find cyber criminals, as well as its legality and its possible rate of effectiveness, are worth investigating; any addition to the arsenal of tools that can be used to expose cyber criminals is valuable.

The importance of always staying one step ahead of "black hat" hackers should come as no surprise to the cybersecurity community. The broad accusation tactic, therefore, because it combines behavioral manipulation with large-scale attacks against potential enemies, could help generate leads as to which questionable individuals are worth investigating further. In other words, a blast accusation email to potential criminals might not solve cyber crimes altogether, but it may help get a better idea of which suspects are more likely to be guilty than others, giving cybersecurity specialists and teams a head start on determining which suspicious actors are truly up to no good based on their response to the accusatory email.

---

[1] Mike Magnoli, "New scam targets cheating husbands with Bitcoin ransom," CW18 Milwaukee, January 25, 2018, http://cw18milwaukee.com/news/offbeat/new-scam-targets-cheating-husbands-with-bitcoin-ransom.

If a cybersecurity team has a list of suspected criminals and any means of contacting them, the broad accusation tactic could be applied and used very easily. Simply gather a list of individuals suspected of committing a certain type of cyber crime (of which there are many, grouped relatively specifically - it would be useless to accuse a malware-related suspect of phishing) and craft an email to send to them all that seems personal and genuine, saying that the authorities are soon to catch the suspect, and outlining a series of steps to take in order to prevent this from happening.

The exact contents of the email can obviously vary, but the theme that the current cheating-spouse blackmail letters are adopting[2] is that of a disgruntled personal investigator who is willing to accept money to stop investigating the cheater. This could be translated into an email intended for the cyber crime suspects in the form of a disgruntled NSA or CIA employee, who is writing to the suspects to inform them that they are being tracked, and offering to delete the personal file of the suspect if they reply requesting the deletion. Then, if the suspect writes back, or if they are being monitored and they start to exhibit track-covering behavior (deleting records, logs, etc.), they can be marked for further investigation by the cybersecurity team.

Of course, there are many other possible ways to craft this email to suspects. They can be very serious or very casual, but should always appear genuine. See Dave Eargle's blog post[3] for the cheating blackmail already used in the real world as a starting point.

The mass-accusation tactic for highlighting potential cyber criminals, while powerful as a tool for any investigator, is not without complications. The first and most important is the its legality and viability in court. According to the US Code of Laws, "A confession . . . shall be admissible in evidence if it is voluntarily given,"[4] meaning that any confession given as a result of the email could be legally valid, but the same code of laws also states that "The trial judge in determining the issue of voluntariness shall take into consideration . . . whether or not such defendant was advised or knew that he was not required to make any statement and that any such statement could be used against him."[5] This means that anybody who admits to a crime via this accusation process could argue in court that they were unaware of the legal gravity of their admission. So, legally speaking, blast accusations are a gray area and the they probably shouldn't be used by people who want to be as legal as possible. However, for actors who are less concerned about being entirely legal, such as United States

---

[2] Dave Eargle, "I received a blackmail letter," Dave Eargle (blog), October 24, 2016, https://daveeargle.com/2016/10/24/I-received-a-blackmail-letter/.
[3] Ibid.
[4] 18 U.S. Code § 3501 - Admissibility of confessions, https://www.law.cornell.edu/uscode/text/18/3501.
[5] Ibid.

government, for example,[6] the legality of mass accusations should not take it out of the question as a usable tactic.

The second issue that this method faces is its functionality. While it may work on some suspects, convincing them to admit to their crimes, it might not work on others. Who are the viable candidates for this sort of investigation, and how many times can mass accusations work before the cybersecurity field as a whole learns to not trust any accusatory email? The answers to these questions, unfortunately, are not nearly as clear-cut as the legal ones discussed in the last paragraph, but my general theory is this: in a world where many types of cyber criminals exist, the most effective target for this tactic is first-time offenders who are less skilled and less likely to know the way cybercrime prevention and criminal justice work. Their ignorance could be used against them, and their lack of experience committing cyber crimes could make them more likely to admit guilt when accused. Advanced cyber criminals, on the other hand, will probably not fall for a broad accusation, and such an accusation might actually make them delete valuable evidence and close down any possibility for accusation in the future. As with all investigation techniques, then, this one should be used with discretion and caution.

Overall, this investigation tactic is worth looking into as a possible first step toward determining the guilt of cyber criminals, and it may also work as a deterrent for anybody just getting into illegal activity - for a new “script kiddie,” a scary, official-looking email from “the government” might motivate them to stop, even if the government doesn’t actually know whether they’re doing anything illegal. In all, though, it’s important to be careful with a tactic like this, because it’s questionable in a legal setting and may only worsen relationships between cybersecurity groups and the criminals they are trying to understand and take down. Like many tools in the field of cybersecurity, this one is a double-edged sword that should be used with caution, but if it can help in staying one step ahead of cyber criminals, it is a tactic that is worthy of consideration.

---

[6] Ariane de Vogue, “Court rules NSA program illegal,” CNN, May 7, 2015, https://www.cnn.com/2015/05/07/politics/nsa-telephone-metadata-illegal-court/index.html.