TWITTER ONLY HAD SMS 2FA WHEN HAL MARTIN'S TWITTER ACCOUNT DMED KASPERSKY

In a post late last month, I suggested that the genesis of FBI's interest in Hal Martin may have stemmed from a panicked misunderstanding of DMs Martin sent.

> What appears to have happened is that the FBI totally misunderstood what it was looking at (assuming, as the context seems to suggest, that this is a DM, it would be an account they were already monitoring closely), and panicked, thinking they had to stop Martin before he dropped more NSA files.

Kim Zetter provides the back story — or at least part of one. The FBI didn't find the DMs on their own. Amazingly, Kaspersky Lab, which the government has spent much of the last four years demonizing, alerted NSA to them.

As Zetter describes, the DMs were cryptic, seemingly breaking in mid-conversation. The second set of DMs referenced the closing scenes of both the 2016 version of Jason Bourne and Inception.

> The case unfolded after someone who U.S. prosecutors believe was Martin used an anonymous Twitter account with the name "HAL999999999" to send five cryptic, private messages to two researchers at the Moscow-based security firm. The messages, which POLITICO has obtained, are brief, and the communication ended altogether as abruptly as it began. After each researcher responded to the confusing messages, HAL999999999 blocked

> their Twitter accounts, preventing them from sending further communication, according to sources.
>
> The first message sent on Aug. 13, 2016, asked for him to arrange a conversation with “Yevgeny” — presumably Kaspersky Lab CEO Eugene Kaspersky, whose given name is Yevgeny Kaspersky. The message didn’t indicate the reason for the conversation or the topic, but a second message following right afterward said, “Shelf life, three weeks,” suggesting the request, or the reason for it, would be relevant for a limited time.
>
> The timing was remarkable — the two messages arrived just 30 minutes before an anonymous group known as Shadow Brokers began dumping classified NSA tools online and announced an auction to sell more of the agency’s stolen code for the price of $1 million Bitcoin. Shadow Brokers, which is believed to be connected to Russian intelligence, said it had stolen the material from an NSA hacking unit that the cybersecurity community has dubbed the Equation Group.
>
> [snip]
>
> The sender’s Twitter handle was not familiar to the Kaspersky recipient, and the account had only 104 followers. But the profile picture showed a silhouette illustration of a man sitting in a chair, his back to the viewer, and a CD-ROM with the word TAO2 on it, using the acronym of the NSA’s Tailored Access Operations. The larger background picture on the profile page showed various guns and military vehicles in silhouette.
>
> The Kaspersky researcher asked the sender, in a reply message, if he had an email address and PGP encryption key

> they could use to communicate. But instead of responding, the sender blocked the researcher's account.
>
> Two days later, the same account sent three private messages to a different Kaspersky researcher.
>
> "Still considering it..," the first message said. When the researcher asked, "What are you considering?" the sender replied: "Understanding of what we are all fighting for … and that goes beyond you and me. Same dilemma as last 10 min of latest Bourne." Four minutes later he sent the final message: "Actually, this is probably more accurate" and included a link to a YouTube video showing the finale of the film "Inception."

As it is, it's an important story. As Zetter lays out, it makes it clear the NSA didn't — couldn't — find Martin on its own, and the government kept beating up Kaspersky even after they helped find Martin.

But, especially given the allusions to the two movies, I wonder whether these DMs actually came from Martin at all. There's good reason to wonder whether they actually come from Shadow Brokers directly.

Certainly, that'd be technically doable, even though court filings suggest Martin had far better operational security than your average target. It would take another 16 months before Twitter offered Authenticator 2 factor authorization. For anyone with the profile of Shadow Brokers, it would be child's play to break SMS 2FA, assuming Martin used it.

Moreover, the message of the two allusions fits solidly within both the practice of cultural allusions as well as the themes employed by Shadow Brokers made over the course of the operation, allusions that have gotten far too little notice.

Finally, that Kaspersky would get DMs from someone hijacking Martin's account would be consistent with other parts of the operation. From start to finish, Shadow Brokers used Kaspersky as a foil, just like it used Jake Williams. With Kaspersky, Shadow Brokers repeatedly provided reason to think that the security company had a role in the leak. In both cases, the government clearly chased the chum Shadow Brokers threw out, hunting innocent people as suspects, rather than looking more closely at what the evidence really suggested. And (as Zetter lays out), Martin would be a second case where Kaspersky was implicated in the identification of such chum, the other being Nghia Pho (the example of whom might explain why the government responded to Kaspersky's help in 2016 with such suspicion).

Mind you, there's nothing in the public record — not Martin's letter asking for fully rendered versions of his social media so he could prove the context, and not Richard Bennett's opinion ruling the warrants based off Kaspersky's tip were reasonable, even if the premise behind them proved wrong — that suggests Martin is contesting that he sent those DMs. That said, virtually the entire case is sealed, so we wouldn't know (and the government really wouldn't want us to know if it were the case).

As Zetter also lays out, Martin had a BDSM profile that might have elicited attention from hostile entities looking for such chum.

> A Google search on the Twitter handle found someone using the same Hal999999999 username on a personal ad seeking female sex partners. The anonymous ad, on a site for people interested in bondage and sado-masochism, included a real picture of Martin and identified him as a 6-foot-4-inch 50-year-old male living in Annapolis, Md. A different search led them to a LinkedIn profile for Hal Martin, described as a researcher in

> Annapolis Junction and “technical advisor and investigator on offensive cyber issues.” The LinkedIn profile didn’t mention the NSA, but said Martin worked as a consultant or contractor “for various cyber related initiatives” across the Defense Department and intelligence community.

And when Kaspersky’s researchers responded to Martin’s DM, he blocked their accounts, suggesting he treated the communications unfavorably (or, if someone had taken over the account, they wanted to limit any back-and-forth, though Martin would presumably have noted that).

> After each researcher responded to the confusing messages, HAL999999999 blocked their Twitter accounts, preventing them from sending further communication, according to sources.

Martin’s attorneys claim he has a mental illness that leads him to horde things, which is the excuse they give for his theft of so many government files. That’s different than suggesting he’d send strangers out-of-context DMs that, at the very least, might make him lose his clearance.

So I’d like to suggest it’s possible that Martin didn’t send those DMs.