FBI'S 26-DAY OLD OPM FLASH NOTICE

Shane Harris, who has been closely tracking the bureaucratic implications of the OPM hack, has an update describing a "FLASH" notice FBI just sent out to the private sector.

Or rather, FBI just re-sent the FLASH notice they sent on June 5, 26 days earlier, because they realized some recipients (including government contractors working on classified projects) did not have their filters set to accept such notices from the FBI.

> The FBI is warning U.S. companies to be on the lookout for a malicious computer program that has been linked to the hack of the Office of Personnel Management. Security experts say the malware is known to be used by hackers in China, including those believed to be behind the OPM breach.
>
> The FBI warning, which was sent to companies Wednesday, includes so-called hash values for the malware, called Sakula, that can be used to search a company's systems to see if they've been affected.
>
> The warning, known as an FBI Liaison Alert System, or FLASH, contains technical details of the malware and describes how it works. While the message doesn't mention the OPM hack, the Sakula malware is used by Chinese hacker groups, according to security experts. And the FBI message is identical to one the bureau sent companies on June 5, a day after the Obama administration said the OPM had been hacked, exposing millions of government employees' personal information. Among the recipients of both alerts are government contractors

> working on sensitive and classified projects.
>
> [snip]
>
> In an email obtained by The Daily Beast, the FBI said it was sending the alert again because of concerns that not all companies had received it the first time. Apparently, some of their email filters weren't configured to let the FBI message through.

Consider the implications of this.

It is unsurprising that the initial FLASH got stuck in companies' email filters if the hashes included with the notice were treated as suspicious code by the companies' anti-malware screens. The message likely looked like malware because it is. (Of course, this story may now have alerted those trying to hack recipients of FBI's FLASH notices that the FBI wasn't previously whitelisted by recipients, but probably just got whitelisted, but that's a matter for another day.)

The delayed FLASH receipt says far more about the current state of data-sharing, just as the Senate sets to debate the Cybersecurity Information Sharing Act, which (Senate boosters claim) companies ostensibly need before they're willing to share data with the government.

First, it suggests that FBI either did not send out such a FLASH in response to what it learned from Anthem hack, which presumably would have gone out at least by February (which, if even OPM had acted on the alert, might have identified its hack 2 months before it did get identified), or if it did it also got stuck in companies' — and OPM's — malware filter.

But it also seems to suggest that the private sector — *including sensitive government contractors* — haven't been receiving other FBI FLASHes (presuming the filter settings have been set to exclude any such notice including

something that looked like malware). They either never noticed they weren't getting them or never bothered to set their filters to receive them.

That may reflect a larger issue, though. As Jennifer Granick has repeatedly noted, key researchers and corporations have not, up to now anyway, seen much value in sharing with the government.

> I've been told by many entities, corporate and academic, that they don't share with the government because the government doesn't share back. Silicon Valley engineers have wondered aloud what value DHS has to offer in their efforts to secure their employer's services. It's not like DHS is setting a great security example for anyone to follow. OPM's Inspector General warned the government about security problems that, left unaddressed, led to the OPM breach.

Perhaps recipients didn't have their filters set to accept notices from FBI because none of them have ever been useful?

Another factor behind reluctance to share with the government is an unwillingness to get personnel security clearances, though that should not be a factor here.

The implication appears to be, though, that the government was unable — because of recipient behavior and predispositions — to share information on the most important hack of recent years.

We're about to have a debate about immunizing corporations further, as if that's the problem. But this delayed FLASH strongly suggests it is not.