BULK COLLECTION IS ALL FUN AND GAMES UNTIL OFFICE OF PERSONNEL MANAGEMENT GETS HACKED

Reuters reports that, contrary to initial reports, the Office of Personnel Management hack revealed earlier this week did compromise the security clearance and background check information in the data, meaning the hack will be far more valuable as intelligence to set up phishing and other further spying efforts. The hack is believed to have been perpetrated by Chinese hackers, though it is unclear thus far whether or not they are part of the government.

> Data stolen from U.S. government computers by suspected Chinese hackers included security clearance information and background checks dating back three decades, U.S. officials said on Friday, underlining the scope of one of the largest known cyber attacks on federal networks.
>
> [snip]
>
> A total of 2.1 million current U.S. government workers were affected, according to a source familiar with the FBI-led investigation into the incident.
>
> Accusations by U.S. government sources of a Chinese role in the cyber attack, including possible state sponsorship, could further strain ties between Washington and Beijing. Tensions are already heightened over Chinese assertiveness in pursuit of territorial claims in the South China Sea.

The same report notes that the hack may be linked to the hack of similar scope of Anthem earlier this year.

This is, as a lot of the current and former government employees I follow on Twitter are realizing this morning, a devastating hack, one which will have repercussions both in the private lives of those whose data has been hacked as well as generally for America's national security, because the data in the OPM servers offers a road map for further espionage targeting.

It is also something the US does all the time — and not just against official government employees of adversary nations, but also against civilian or quasi civilian telecom targets, as well as employees of corporations of interest.

This WaPo piece quotes a number of cybersecurity people suggesting several recent major hacks are being used to pull together large data repositories — similar to in purpose but at this point just a mere shadow of what we do using bulk collection and XKeyscore. But it tries to suggest the Chinese collection of bulk data is worse because, "in China, the authorities do not tolerate public debate over the proper limits of large-scale spying in the digital age."

The US Intelligence Community let us have a debate over a mere fraction of the bulk data being collected by the NSA — that collected domestically to target Americans. But for the stuff targeting foreigners on a far greater scale, President Obama proclaimed we would continue collecting in bulk but limit its use to all the major purposes we were already using it for before we ever got around to debating the Section 215 dragnet.

> (1) espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests;
>
> (2) threats to the United States and its interests from terrorism;

> (3) threats to the United States and its interests from the development, possession, proliferation, or use of weapons of mass destruction;
>
> (4) cybersecurity threats;
>
> (5) threats to U.S. or allied Armed Forces or other U.S or allied personnel;
>
> (6) transnational criminal threats, including illicit finance and sanctions evasion related to the other purposes named in this section.

That scope goes well beyond the scope of those affected in this OPM hack.

Once the government does whatever it can to protect the millions compromised by this hack, I hope it will provide an opportunity to do two things: focus on actual cyber-defense, rather than an offensive approach that itself entails and therefore legitimates precisely this kind of bulk collection, and reflect on whether the world we've built, in which millions of innocent people get swept up in spying because it's easy to do so, is really one we want to pursue. Ideally, such reflection might lead to some norm-setting that sharply limits the kinds of targets who can be bulk collected (though OPM would solidly fit in any imaginable such limits).

China has, unsurprisingly, now adopted our approach, even if it would take a decade for it to catch up in ability to bulk collect from most nodes. And that's going to suck for a lot of government and private sector employees who will be made targets as a result.

But that's the world and the rules we chose to create.

Update: See this NYT piece for just how shoddy the security on OPM's servers was. We've been arguing for years about ways to better respond to criminal hackers and neglecting really really basic steps needed to prevent our adversaries

from adopting the same approach we use.