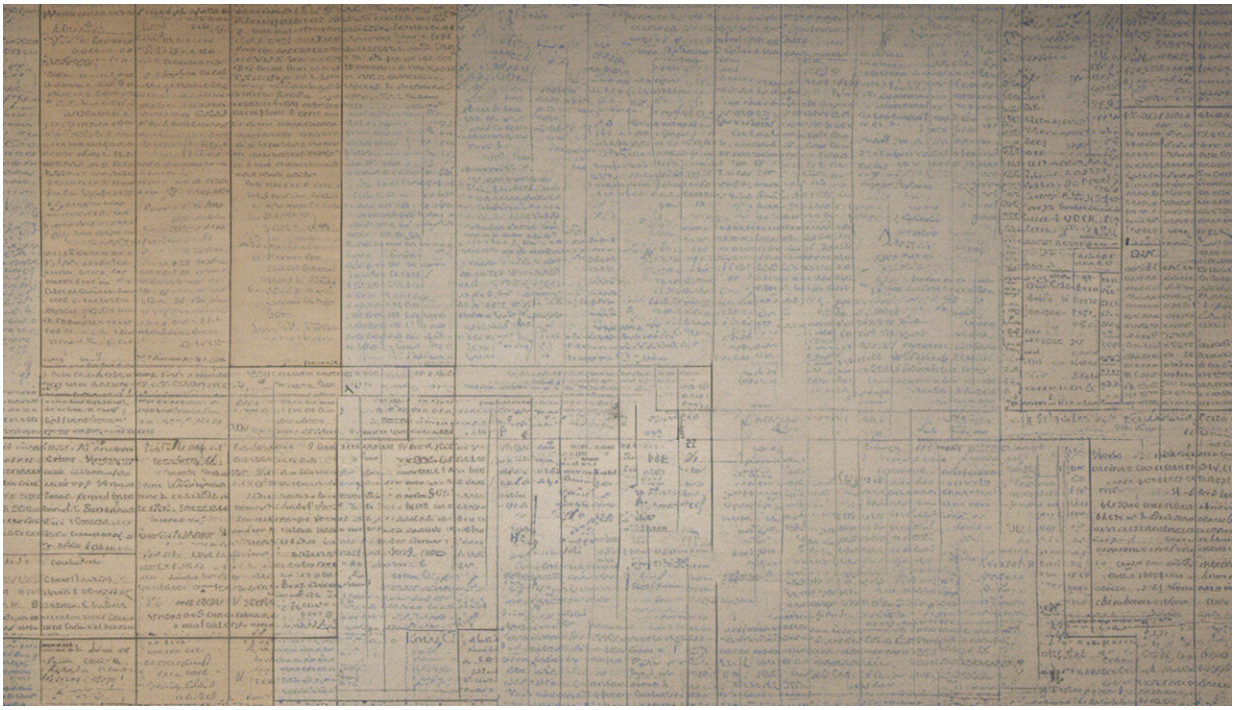
The WikiLeaks CIA release—when will we learn?

March 9 2017, by Richard Forno And Anupam Joshi



Credit: AI-generated image (disclaimer)

This week's WikiLeaks release of what is apparently a trove of Central Intelligence Agency information related to its computer hacking should surprise no one: Despite its complaints of being targeted by cyberattackers from other countries, the U.S. does a fair amount of its own hacking. Multiple federal agencies are involved, including the CIA

and the National Security Agency, and even friendly nations. These latest disclosures also remind us of the cybersecurity truism that any electronic device connected to a network can be hacked.

As cybersecurity researchers conducting a preliminary review of the data released in what WikiLeaks calls "Vault 7," we find the documents mostly confirm existing knowledge about how common hacking is and how many potential targets there are in the world.

This round of leaks, of documents dating from 2013 to 2016, also reinforces perhaps the most troubling piece of information we already knew: Individuals and the government itself must step up cyberdefense efforts to protect sensitive information.

Almost everything is hackable

For years, security experts and researchers have warned that if something is connected to the internet it is vulnerable to attack. And spies around the world routinely gather intelligence electronically for diplomatic, economic and national security purposes.

As a result, we and others in the cybersecurity community were not surprised by the 2013 revelations from former NSA contractor Edward Snowden. We knew that the spying programs he disclosed were possible if not likely. By contrast, the general public and many politicians were astounded and worried by the Snowden documents, just as many citizens are surprised by this week's WikiLeaks disclosure.

One element of the new WikiLeaks "Vault 7" release provides more insight into the scope of government spying. In a project called "Weeping Angel," CIA hackers and their U.K. counterparts worked to turn Samsung F8000 smart television sets into remote surveillance tools. Hacked TV's could record what their owners said nearby, even when

they appeared to be turned off.

The fact that the CIA specifically targeted smart televisions should serve as yet another a wake-up call to the general public and technology manufacturers about cybersecurity issues inherent in modern devices. Specifically, "smart home" and Internet of Things devices represent a massive vulnerability. They are open to attack not only by government organizations seeking intelligence on national security information, but terrorists, criminals or other adversaries.

It's not necessarily a good idea to have always-on and network-enabled microphones or cameras in every room of the house. Despite many of these devices being sold with insecure default settings, the market is growing very rapidly. More and more people are buying Google Home or Amazon Echo devices, Wi-Fi enabled baby monitors and even internet-connected home-security equipment.

These have already caused problems for families whose devices overheard a TV newscaster and ordered dollhouses or whose kids were tracked by a teddy bear. And large parts of the internet were disrupted when many "smart" devices were hijacked and used to attack other networked systems.

Phones were a key target

The CIA also explored ways to take control of smartphone operating systems, allowing the agency to monitor everything a phone's user did, said or typed on the device. Doing so would provide a way around post-Snowden encrypted communications apps like WhatsApp and Signal. However, some of the CIA's methods of attack have already been blocked by technology vendors' security updates.

The CIA's apparent ability to hack smartphones casts doubt on the need

for officials' repeated calls to weaken mobile phone encryption features. It also weakens the government's claim that it must strengthen surveillance by not telling tech companies when it learns of security weaknesses in everyday products. Just like the door to your house, technological vulnerabilities work equally well in providing access to both "good guys" and "bad guys."

Ultimately, as a society, we must continue to debate the trade-offs between the conveniences of modern technologies and security/privacy. There are definite benefits and conveniences from pervasive and wearable computing, smart cars and televisions, internet-enabled refrigerators and thermostats, and the like. But there are very real security and privacy concerns associated with installing and using them in our personal environments and private spaces. Additional problems can come from how our governments address these issues while respecting popular opinion and acknowledging the capabilities of modern technology.

As citizens, we must decide what level of risk we – as a nation, a society and as individuals – are willing to face when using internet-connected products.

We're frequent attackers – but bad defenders

The WikiLeaks release also reconfirms a reality the U.S. might prefer to keep quiet: While the government objects to others' offensive cyberattacks against the United States, we launch them too. This isn't news, but it hurts America's reputation as a fair and aboveboard player on the international stage. It also also reduces American officials' credibility when they object to other countries' electronic activities.

Leaks like this reveal America's methods to the world, providing plenty of direction for adversaries who want to replicate what government

agents do – or even potentially launch attacks that appear to come from American agencies to conceal their own involvement or deflect attribution.

But perhaps the most disturbing message the WikiLeaks disclosure represents is in the leak itself: It's another high-profile, high-volume breach of information from a major U.S. government agency – and at least the third significant one from the secretive intelligence community.

Perhaps the largest U.S. government data loss incident was the 2014 Office of Personnel Management breach that affected more than 20 million current and former federal workers and their families (including this article's authors). But the U.S. has never truly secured its digital data against cyberattackers. In the 1990s there was Moonlight Maze; in the 2000s there was Titan Rain. And that's just for starters.

Our government needs to focus more on the mundane tasks of cyberdefense. Keeping others out of key systems is crucial to American national security, and to the proper function of our government, military and civilian systems.

Achieving this is no easy task. In the wake of this latest WikiLeaks release, it's certain that the CIA and other agencies will further step up their insider-threat protections and other defenses. But part of the problem is the amount of data the country is trying to keep secret in the first place.

We recommend the federal government review its classification policies to determine, frankly, if too much information is needlessly declared secret. Reportedly, as many as 4.2 million people – federal employees and contractors – have security clearances. If so many people need or are given access to handle classified material, is there just too much of it to begin with? In any case, the information our government declares secret

is available to a very large group of people.

If the U.S. is going to be successful at securing its crucial government information, it must do a better job managing the volume of information generated and controlling access to it, both authorized and otherwise. Granted, neither is an easy task. However, absent fundamental changes that fix the proverbial cult of classification, there likely will be many more WikiLeaks-type disclosures in the future.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation

Citation: The WikiLeaks CIA release—when will we learn? (2017, March 9) retrieved 8 May 2024 from https://phys.org/news/2017-03-wikileaks-cia-releasewhen.html