# Report: CIA received more offensive hacking powers in 2018

By Written by Catalin Cimpanu, ContributorContributor July 15, 2020 at 6:07 a.m. PT




CIA headquarters in Langley, VA. (Image: file photo)

BRENDAN SMIALOWSKI/AFP/Getty Images

## Special feature

US President Donald Trump gave broad powers to the Central Intelligence Agency (CIA) in 2018 to carry out offensive cyber operations across the globe.

In an exclusive today, Yahoo News reported that the agency used its newly acquired powers to orchestrate "at least a dozen operations" across the world.

The CIA was already authorized to conduct silent surveillance and data collection, but the new powers allow it to go even further.

"This has been a combination of destructive things - stuff is on fire and exploding - and also public dissemination of data: leaking or things that look like leaking," a former US government official told Yahoo News.

While the former official didn't go into the specifics of each operation, Yahoo News reporters believe the CIA's new powers and modus operandi link it to a series of hack-and-dump incidents that took place primarily in 2019, such as:

- Publishing hacking tools (malware) from APT34, an Iranian government hacking unit, on Telegram.
- Doxing Islamic Revolutionary Guard Corps (IRGC) intelligence agents on Telegram by revealing their full names, home addresses, phone numbers, and social media profiles.
- Dumping details about 15 million payment cards from three Iranian banks linked to Iran's IRGC.
- Hacking two contractors that provide cyber-weapons and surveillance solutions for Russia's FSB intelligence agency and sharing the data online via a hacktivist group called Digital Revolution.

Citing former US officials, Yahoo News claims that such operations would have never been approved in the previous administrations, who have always been very cautious when attacking foreign adversaries, fearing blowback.

However, in 2018, President Trump departed from the White House's classic stance on the matter and signed a document called a presidential finding, granting the CIA the ability to plan and execute covert offensive cyber operations under its judgment, rather than under the oversight of the National Security Council.

The document effectively took the decision making and approval process from the White House and the National Security Council and placed it with CIA leadership in an attempt to expedite foreign hacking operations.

Yahoo News reports that President Trump's decision split top US intelligence officials.

Some officials feared repercussions from foreign adversaries, while some feared the lack of NSC oversight. NSC oversight previously kept US intelligence agencies like the CIA in check when it came to orchestrating and approving cyber operations on foreign ground, making sure agencies like the NSA and CIA went through a due process that would sometime take years from the planning to the execution phase.

However, Yahoo News sources said that some intelligence officials were ecstatic at Trump's decision, calling it "a needed reform" in order to make the CIA more agile and speed up response times to foreign attacks.

The locations of these foreign CIA cyber operations are currently classified, along with operational details, but former US officials who have seen the presidential finding said the document listed Russia, China, Iran, and North Korea as targets, but also left the door open for the CIA to carry out operations in other countries at its discretion.

*Article title updated to reflect the original report better.*

**The world's most famous and dangerous APT (state-developed) malware**

**Security**

Editorial standards

---