# US government is now the biggest buyer of malware, Reuters reports

www.theverge.com/2013/5/10/4319278/us-government-hacking-threatens-cybersecurity-former-officials-say

The US government is waging electronic warfare on a vast scale — so large that it's causing a seismic shift in the unregulated grey markets where hackers and criminals buy and sell security exploits, Reuters reports.

Former White House cybersecurity advisors Howard Schmidt and Richard Clarke say this move to "offensive" cybersecurity has left US companies and average citizens vulnerable, because it relies on the government collecting and exploiting critical vulnerabilities that have not been revealed to software vendors or the public.

"If the US government knows of a vulnerability that can be exploited, under normal circumstances, its first obligation is to tell US users," Clarke told Reuters. "There is supposed to be some mechanism for deciding how they use the information, for offense or defense. But there isn't."

""My job was to have 25 zero-days on a USB stick, ready to go." "

Vulnerabilities go for a pretty penny in the computer hacking underground — zero-day exploits (those which are unknown to software developers at the time of discovery) have been known to sell for as much as $50,000 - $100,000 each. Once obtained, these exploits are packaged into weaponized malware and sold to criminals and repressive governments across the world, who then use it to do everything from spying on citizens to conducting cyber espionage against rival nations and companies — or, in the case of the US / Israel-backed Stuxnet worm, destroying industrial machinery inside an Iranian nuclear facility. One former executive for a defense contractor described his job as "to have 25 zero-days on a USB stick, ready to go" so that governments could use them as cyber weapons.

The US government won't say anything about the scope or details of its cyber warfare efforts, but vendors and former defense contractors say the US has become a top buyer in the burgeoning malware market. Former officials worry that this shift in priorities is luring skilled hackers and researchers away from defense and toward the more lucrative business of building weaponized malware for government use.

"There has been a traditional calculus between protecting your offensive capability and strengthening your defense," said former NSA director Michael Hayden. "It might be time now to readdress that at an important policy level, given how much we are suffering."