Wikileaks: The CIA is using popular TVs, smartphones and cars to spy on their owners

By Craig Timberg, Ellen Nakashima and Elizabeth Dwoskin March 7, 2017

The latest revelations about U.S. government’s powerful hacking tools potentially takes surveillance right into the homes and hip pockets of billions of users worldwide, showing how a remarkable variety of every day devices can be turned to spy on their owners.

Televisions, smartphones and Internet-connected vehicles are all vulnerable to CIA hacking, according to the Wikileaks documents released Tuesday. The capabilities described include recording the sounds, images and the private text messages of users, even when they use encrypted apps to communicate. The CIA also studied whether it could infect vehicle control systems used by modern cars and trucks, which Wikileaks said could allow “nearly undetectable assassinations.”

In the case of a tool called “Weeping Angel” for attacking Samsung SmartTVs, Wikileaks wrote, “After infestation, Weeping Angel places the target TV in a 'Fake-Off' mode, so that the owner falsely believes the TV is off when it is on, In 'Fake-Off' mode the TV operates as a bug, recording conversations in the room and sending them over the Internet to a covert CIA server.”

The documents, which The Washington Post could not independently verify and the CIA has declined to confirm, list supposed tools for cracking into such widely popular devices as Apple’s iPhone or the Android smartphones whose operating system is made by Google, but there are marked differences from the 2013 revelations by the National Security Agency’s former contractor Edward Snowden.

His documents largely described mass surveillance of Internet-based communications systems, more often than the individual devices that appear to have been the focus of the CIA. By targeting devices, the CIA could gain access to even well-encrypted communications, on such popular apps as Signal and WhatsApp, without having to crack the encryption itself. The Wikileaks reports appear to acknowledge that difference by saying the CIA “bypassed” as opposed to defeated encryption technologies.

Resignation and frustration rippled through Silicon Valley on Tuesday as technologists grappled with revelations of yet another government attempt to exploit their systems.

“The argument that there is some terrorist using a Samsung TV somewhere – as a reason to not disclose that vulnerability to the company, when it puts thousands of Americans at risk — I fundamentally disagree with it, “said Alex Rice, chief technology officer for Hacker One, a startup that enlists hackers to report security gaps to companies and organizations in exchange for cash.

Privacy experts say the CIA may have been forced into focusing on vulnerable devices because the Internet overall has become more secure through more widespread deployment of encryption. In this new world, devices have become the most vulnerable link.

“The idea that the CIA and NSA can hack into devices is kind of old news,” said Johns Hopkins cryptography expert Matthew Green. “Anyone who thought they couldn’t was living in a fantasy world.”

Snowden’s revelations and the backlash made strong encryption a major, well-funded cause for both privacy advocates and, perhaps more importantly, technology companies that had the engineering expertise and budgets to protect data as it flowed across the world.

Google, Microsoft, Facebook, Yahoo and many other companies announced major new initiatives, in part to protect their brands against accusations by some users that they had made it too easy for the NSA to collect information from their systems. Many Web sites, meanwhile, began encrypting their data flows to users to prevent snooping. Encryption tools such as Tor were strengthened.

Encrypting apps for private messaging, such as Signal, Telegram and WhatsApp exploded in popularity, especially among users around the world who were fearful of government intrusion. In the days following the U.S. presidential election, Signal was among the most downloaded in Apple's app store and downloads grew by more than 300 percent.

Open Whispers Systems, which developed Signal, released a statement: "The CIA/Wikileaks story today is about getting malware onto phones, none of the exploits are in Signal or break Signal Protocol encryption." WhatsApp declined to comment, and Telegram did not respond to requests for comment. Google declined to comment, while Samsung and Apple did not immediately respond to requests for comment.

U.S. government authorities complained loudly that the new wave of encryption was undermining their ability to investigate serious crimes, such as terrorism and child pornography. The FBI sued Apple in hopes of forcing it to unlock an iPhone used by the San Bernadino killers before announcing it had other ways to crack the device amid heavy public criticism.

Against that backdrop, many privacy advocates argued that devices — often called “endpoints” for their place on chains of communications that can criss-cross continents — were the best available target left in a world with widespread online encryption. The Wikileaks documents suggests that the CIA may have reached the same conclusion.

“It would certainly be consistent with the hypothesis that we’ve made real progress in the encryption we’ve been introducing,” said Peter Eckersley, technology projects director for the Electronic Frontier Foundation, a San Francisco-based civil liberties group. “It’s impossible to be 100 percent certain, but reading the tea leaves, it’s plausible.”

The Wikileaks revelations also will serve as a reminder that, for whatever the political backlash to revelations about digital spying, it is not going away and probably will continue to grow. The focus on hacking into individual devices -- rather than the messages traveling between them -- is likely to increase pressure on companies to make those devices safer because, as experts have long said, they are the most vulnerable target in a long chain of digital interactions.

That could be especially important for U.S. tech companies, such as Google, Apple and Facebook, that have worked to rebuild their reputations as stewards of their users' privacy in recent years.

Cybersecurity experts, meanwhile, reacted with alarm to the news of the Wikileaks release.

“This is explosive,” said Jake Williams, founder of Rendition Infosec, a cybersecurity firm. The material highlights specific antivirus products that can be defeated, going further than a release of NSA hacking tools last year, he said.

The CIA hackers, according to WikiLeaks, even “discussed what the NSA's …hackers did wrong and how the CIA's malware makers could avoid similar exposure.”

Hackers who worked at NSA's Tailored Access Operations unit said the CIA's library of tools looked comparable. The description of the implants, which are software that enable a hacker to remotely control a compromised device, and other attack tools appear to be “very, very complex” and “at least on par with the NSA,” said one former TAO hacker who spoke on condition his name not be used.

The WikiLeaks release revealed that they have sophisticated “stealth” capabilities that enable hackers not only to infiltrate systems, but evade detection, as well as abilities to “escalate privileges” or move inside a system as if they owned it.

“The only thing that separates NSA from commodity malware in the first place is their ability to remain hidden,” the former TAO hacker said. “So when you talk about the stealth components, it's huge that you're seeing a tangible example here of them using and researching stealth.”

Computer security experts noted that the release includes no actual tools or exploits, “so we don't know if WikiLeaks did not get them or is just not choosing to publish them,” Nicholas Weaver, a computer security researcher at the University of California at Berkeley. “However we should assume that whoever stole this data has access to the exploits and tools.”

He noted that the dates in the files suggest the tools were taken in February or March 2016 and that there are at least two documents marked Top Secret, “which suggests that somebody in early 2016 managed to compromise a Top Secret CIA development system and is willing to say that they did.”

One internal CIA document listed a set of Apple iPhone “exploits” — or tools that can be used to compromise the device by taking advantage of software flaws. Some of the tools are based on “zero-days,” which are software vulnerabilities that have not been shared with the manufacturer. So “some of these descriptions will allow Apple to fix the vulnerabilities,” Weaver said. “But at the same time, they’re out in the public and whoever stole this data could use them against U.S. interests.”