PHYS.ORG

WikiLeaks aid on CIA software holes could be mixed blessing

March 10 2017, by Anick Jesdanun And Michael Liedtke

WikiLeaks founder Julian Assange speaks in this video made available Thursday March 9, 2017. Assange said his group will work with technology companies to help defeat the Central Intelligence Agency's hacking tools. Assange says "we have decided to work with them, to give them some exclusive access to some of the technical details we have, so that fixes can be pushed out." (WikiLeaks via AP)

WikiLeaks has offered to help the likes of Google and Apple identify the software holes used by purported CIA hacking tools—and that puts the tech industry in something of a bind.

While companies have both a responsibility and financial incentive to fix problems in their software, accepting help from WikiLeaks raises legal and ethical questions. And it's not even clear at this point exactly what kind of assistance WikiLeaks can offer.

THE PROMISE

WikiLeaks founder Julian Assange said Thursday that the anti-secrecy site will help technology companies find and fix software vulnerabilities in everyday gadgets such as phones and TVs. In an online news conference, Assange said some companies had asked for more details about the purported CIA cyberespionage toolkit that he revealed in a massive disclosure on Tuesday.

"We have decided to work with them, to give them some exclusive access to the additional technical details we have, so that fixes can be developed and pushed out," Assange said. The digital blueprints for what he described as "cyberweapons" would be published to the world "once this material is effectively disarmed by us."

Any conditions WikiLeaks might set for its cooperation weren't immediately known. Nor was it clear if WikiLeaks holds additional details on specific vulnerabilities, or merely the tools designed to exploit them.

Apple declined comment on the WikiLeaks offer, and Google didn't respond to requests for comment. Microsoft said it hopes that anyone with knowledge of software vulnerabilities would report them through the company's usual channels.

This April 13, 2016, file photo shows the seal of the Central Intelligence Agency at CIA headquarters in Langley, Va. An alleged CIA surveillance program disclosed by WikiLeaks on Tuesday, March 7, 2017, purportedly targeted security weaknesses in smart TVs, smartphones, personal computers and even cars, and enabled snooping that could circumvent encryption on communications apps such as Facebook's WhatsApp. WikiLeaks is, for now, withholding details on the specific hacks used. But WikiLeaks claims that the data and documents it obtained reveal a broad program to bypass security measures on everyday products. (AP Photo/Carolyn Kaster, File)

LEGAL QUESTIONS

Tech companies could run into legal difficulties in accepting the offer, especially if they have government contracts or employees with security clearances.

"The unauthorized release of classified documents does not mean it's unclassified," said Stewart Baker, a former official at the Department of Homeland Security and former legal counsel for the National Security Agency. "Doing business with WikiLeaks and reviewing classified documents poses a real risk for at least their government contracting arms and their cleared employees."

Other lawyers, however, are convinced that much of the information in the documents is so widely known that they are now part of the public domain. That means tech companies would be unlikely to face any legal liability for digging deeper with WikiLeaks.

Alternatively, suppose tech companies don't accept WikiLeaks' offer to help fix any security flaws—and are subsequently hacked. At that point, they could face charges of negligence, particularly in Europe where privacy laws are much stricter than in the U.S., said Michael Zweiback, a former assistant U.S. attorney and cybercrime adviser now in private practice.

GETTING TOO CLOSE TO WIKILEAKS

Public perception might be a bigger problem. "They don't want to be seen as endorsing or supporting an organization with a tainted reputation and an unclear agenda," said Robert Cattanach, a former U.S. Department of Justice attorney.

During the 2016 election, WikiLeaks published thousands of emails, some embarrassing, from breached Democratic Party computers and the account of a top aide to Hillary Clinton. U.S. intelligence agencies concluded those emails were stolen by hackers connected to the Russian government in an attempt to help Donald Trump win the presidency.

The CIA did not respond directly to Assange's offer, but it appeared to take a dim view of it.

"Julian Assange is not exactly a bastion of truth and integrity," CIA spokeswoman Heather Fritz Horniak said.

But most tech companies already have digital hotlines to receive tips about security weaknesses, even if they come from unsavory characters. So it wouldn't break new ground for them to consult with a shadowy organization such as WikiLeaks.

This Feb. 19, 2014, file photo, shows WhatsApp and Facebook app icons on a smartphone in New York. So, you use messaging apps like WhatsApp or Signal or have smart TVs and PCs. Should you worry that the CIA is listening to your conversations? The short answer is no. The long answer is maybe, but it's unlikely. Revelations by WikiLeaks describing secret CIA hacking tools the government uses to break into computers, mobile phones and even smart TVs, if true, could certainly have real-life implications for anyone who uses internet-connected technology.(AP Photo/Patrick Sison, File)

A BETTER PATH

Ideally, the CIA would have shared such vulnerabilities directly with companies, as other government agencies have long done. In that case, companies would not only be dealing with a known entity in an aboveboard fashion, they might also obtain a more nuanced understanding of the problems than their engineers could glean from documents or lines of computer code.

And if companies could learn details about how the CIA found these vulnerabilities, they might also find additional holes using the same technique, said Johannes Ullrich, director of the Internet Storm Center at the SANS Institute.

And there are risks obtaining actual hacking tools from WikiLeaks. Some might have unadvertised features that could, for instance, start extracting data as soon as they launch. Ullrich said the CIA also might have left some traps to attack people running its exploits. If these aren't detailed in the documents, only the CIA would be able to help tech companies avoid setting them off.

If all goes well, WikiLeaks could emerge looking better than some parts of the U.S. government.

"I am not a fan of WikiLeaks, but I don't think it is fair to throw rocks at everything they do," said Cindy Cohn, executive director of the Electronic Frontier Foundation, a group specializing in online privacy and other digital rights. "What WikiLeaks is demonstrating is that the CIA does not have the best interests of these companies at heart."

BETTER THAN NOTHING

There's one more unknown, which is just how much help WikiLeaks can actually provide. Apple, Google and Microsoft say they've already rendered many of the alleged CIA cyberespionage tools obsolete with earlier updates that patched related software holes.

Still, the companies will probably want to check out what WikiLeaks has, assuming that the organization hasn't set unreasonable conditions on its cooperation. Some privacy and security experts believe the CIA's own refusal to contact the affected companies about the vulnerabilities gives them little choice.

"We all should have better security, and certainly at this point, not trying to fixing them makes no sense," Cohn said.

Citation: WikiLeaks aid on CIA software holes could be mixed blessing (2017, March 10) retrieved 10 April 2024 from
https://phys.org/news/2017-03-wikileaks-aid-cia-software-holes.html