WikiLeaks: CIA has targeted everyday gadgets for snooping

March 7 2017, by Anick Jesdanun

This is Thursday, Jan. 12, 2017 file photo of the new CIA Director Michael Pompeo, as he testifies on Capitol Hill in Washington. WikiLeaks has published thousands of documents that it says come from the CIA's Center for Cyber Intelligence, a dramatic release that appears to give an eye-opening look at the intimate details of the agency's cyberespionage effort. (AP Photo/Manuel Balce Ceneta)

Maybe the CIA is spying on you through your television set after all.

Documents released by WikiLeaks allege a CIA surveillance program that targets everyday gadgets ranging from smart TVs to smartphones to cars. Such snooping, WikiLeaks said, could turn some of these devices into recorders of everyday conversations—and could also circumvent data-scrambling encryption on communications apps such as Facebook's WhatsApp.

WikiLeaks is, for now, withholding details on the specific hacks used "until a consensus emerges" on the nature of the CIA's program and how the methods should be "analyzed, disarmed and published." But WikiLeaks—a nonprofit that routinely publishes confidential documents, frequently from government sources—claims that the data and documents it obtained reveal a broad program to bypass security measures on everyday products.

MORE PRIVACY CLASHES

If true, the disclosure could spark new privacy tensions between the government and the technology industry. Relations have been fraught since 2013, when former National Security Agency contractor Edward Snowden disclosed secret NSA surveillance of phone and digital communications.

Just last year, the two sides feuded over the FBI's calls for Apple to rewrite its operating system so that agents could break into the locked iPhone used by one of the San Bernardino attackers. The FBI ultimately broke into the phone with the help of an outside party; the agency has neither disclosed the party nor the nature of the vulnerability, preventing Apple from fixing it.

According to WikiLeaks, much of the CIA program centered on dozens of vulnerabilities it discovered but didn't disclose to the gadget makers. Common practice calls for government agencies to disclose such flaws to

companies privately, so that they could fix them.

Instead, WikiLeaks claims, the CIA held on to the knowledge in order to conduct a variety of attacks. As a result, tech companies such as Apple, Google and Microsoft haven't been able to make the necessary fixes.

"Serious vulnerabilities not disclosed to the manufacturers places huge swathes of the population and critical infrastructure at risk to foreign intelligence or cyber criminals who independently discover or hear rumors of the vulnerability," WikiLeaks wrote in a press release. "If the CIA can discover such vulnerabilities so can others."

A BIG YAWN TO SOME

Not everyone is worried, though.

Alan Paller, director of research for the cybersecurity training outfit SANS Institute, said the case boils down to "spies who use their tools to do what they are paid to do." He said criminals already have similar tools—and he's more worried about that.

Rich Mogull, CEO of the security research firm Securosis, said that agencies gathering intelligence on other organizations and governments need, by definition, technical exploits that aren't public.

If they're authentic, the leaked CIA documents frame a stark reality: It may be that no digital conversation, photo or other slice of life can be shielded from spies and other intruders prying into smartphones, personal computers, tablets or just about device connected to the internet.

"It's getting to the point where anything you say, write or electronically transmit on a phone, you have to assume that it is going to be

compromised in some way," said Robert Cattanach, a former U.S. Department of Justice attorney who now specializes in cybersecurity and privacy for the law firm Dorsey & Whitney.

SIDESTEPPING ENCRYPTION

WikiLeaks claims the hacks allowed the CIA to collect audio and other messages from data-scrambling communication apps such as WhatsApp, Signal, Telegram and Confide by intercepting data before it is encrypted or after it's decoded. The CIA didn't appear to compromise the apps themselves, but rather the phone's underlying operating system.

WikiLeaks says the CIA had separate teams looking for vulnerabilities in iPhones and Android phones and also targeted tablets such as iPads. According to WikiLeaks, the vulnerabilities were discovered by the CIA itself or obtained from other government agencies and cyberweapon contractors.

CARS, TRUCKS AND TVS

WikiLeaks also claims that the CIA worked with U.K. intelligence officials to turn microphones in Samsung smart TVs into listening devices. The microphones are normally there for viewers to make voice commands, such as requests for movie recommendations. If the TV is off, there's no listening being done.

But WikiLeaks claims that a CIA hack makes the target TV appear to be off when it's actually on—and listening. WikiLeaks says the audio goes to a covert CIA server rather than a party authorized by Samsung. In such cases, audio isn't limited to TV commands but could include everyday conversations.

Other tools in the CIA's arsenal target PCs running Microsoft's Windows

system, according to WikiLeaks, which says many of the attacks are in the form of viruses designed to spread through CDs and USB drives.

WikiLeaks also says the CIA was also targeting control systems used by cars and trucks. Although WikiLeaks didn't have details on how that might be used, it said the capability might allow the CIA to "engage in nearly undetectable assassinations."

Microsoft said it was aware of the reports and was looking into them.

Apple said an initial analysis showed many of the security gaps brought up in the leaked documents were already patched in the latest iOS.

"We will continue work to rapidly address any identified vulnerabilities," it said.

Google and Samsung didn't immediately respond to requests for comment. In a statement, General Motors said it would be premature to comment on the documents, including its authenticity. But GM added that it knew of no injuries or death resulting from the hacking of a vehicle.