WikiLeaks CIA files: Are they real and are they a risk?

8 March 2017, by Stephen Braun

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)

WikiLeaks has published thousands of documents that the anti-secrecy organization said were classified files revealing scores of secrets about CIA hacking tools used to break into targeted computers, cellphones and even smart TVs.

The CIA and the Trump administration declined to comment on the authenticity of the files Tuesday, but prior WikiLeaks releases divulged government secrets maintained by the State Department, Pentagon and other agencies that have since been acknowledged as genuine. In another nod to their authenticity, the chairman of the House intelligence committee, Rep. Devin Nunes, R-Calif., said he was very concerned about the release and has sought more information about it.

The hacking tools appeared to exploit vulnerabilities in popular operating systems for desktop and laptop computers developed by Microsoft. They also targeted devices that included Apple's iPhones and iPads, Google's Android cellphones, Cisco routers and Samsung Smart TVs.

Some of the technology firms said they were evaluating the newly released documents.

Some questions and answers about the latest WikiLeaks dump and its fallout:

WHERE DO THESE DOCUMENTS COME FROM?

WikiLeaks said the material came from "an isolated, high-security network" inside the CIA's Center for Cyber Intelligence, the spy agency's internal arm that conducts cyber offense and defense. It said the documents were "circulated among former U.S. government hackers and contractors in an unauthorized manner, one of whom has provided WikiLeaks with portions of the archive." It did not make it clear who was behind the leak, leaving several possibilities: espionage, a rogue employee, a theft involving a federal contractor or a break-in of a staging server where such information may have been temporarily stored.

HOW MANY FILES WERE LEAKED? WHAT PERIOD DO THEY COVER?

WikiLeaks said 7,818 web pages and 943 attachments were published, but were just the first part of more material to come. WikiLeaks said it has an entire archive of data consisting of several million lines of computer code. The documents appear to date between 2013 and 2016. WikiLeaks described them as "the largest-ever publication of confidential documents on the agency."

ARE THESE LEGITIMATE CIA DOCUMENTS?

A spokesman for the CIA said the agency would not comment "on the authenticity or content of purported intelligence documents." Trump administration spokesman Sean Spicer declined comment as well. But WikiLeaks has a long track record of assembling and releasing secret files from the U.S. and other governments. Security experts who reviewed the material said the documents appeared to be authentic. Jake Williams, a security expert with Georgia-based Rendition Infosec, who has dealt previously with government hackers, said that frequent references in the files to operation security gave them the stamp of legitimacy. "It rings true to me," Williams said.

WHAT DO THESE DOCUMENTS CONTAIN?

The files describe CIA plans and descriptions of malware and other tools that could be used to hack into some of the world's most popular technology platforms. The documents showed that the developers aimed to be able to inject these tools into targeted computers without the owners' awareness.

The files do not describe who the prospective targets might be, but the documents show broad exchanges of tools and information between the CIA and National Security Agency and other federal intelligence agencies, as well as intelligence services of close allies Australia, Canada, New Zealand and the United Kingdom.

The purported CIA documents range from complicated computer coding to organizational plans to sarcastic comments about the tools' effectiveness. Some of the tools were named after alcohol references, including Bartender, Wild Turkey and Margarita. Others referenced recent popular movies, including "Fight Club" and "Talladega Nights." One hacking tool, code-named "RickyBobby," after the character who is a race car driver in "Talladega Nights," was purportedly used to upload and download information "without detection as malicious software."

The documents also include discussions about compromising some internet-connected televisions to turn them into listening posts. One document discusses hacking vehicle systems, appearing to indicate the CIA's interest in hacking recent-model cars with sophisticated on-board computer systems.

HOW ARE TECHNOLOGY FIRMS RESPONDING TO THESE REVELATIONS?

Microsoft said it was looking into the reports that its operating systems were potentially vulnerable to many of the malware and other hacking tools described in the purported CIA documents. The maker of the secure messaging app Signal said the purported tools described in the leaked documents appeared to affect users' actual phones, but not its software designs or encryption protocols. The manufacturer of the popular Telegram mobile messaging app said in a statement that manufacturers of cellphones and their operating systems, including Apple, Google and Samsung, were responsible for improving the security of their devices. It said the effort will require "many hours of work and many security updates" and assured its customers that "If the CIA is not on your back, you shouldn't start worrying yet."