WikiLeaks reveals CIA trove alleging wide-scale hacking

March 7 2017, by Jack Gillum And Raphael Satter

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)

WikiLeaks published thousands of documents Tuesday described as

secret files about CIA hacking tools the government employs to break into users' computers, mobile phones and even smart TVs from companies like Apple, Google, Microsoft and Samsung.

The documents describe clandestine methods for bypassing or defeating encryption, antivirus tools and other protective security features intended to keep the private information of citizens and corporations safe from prying eyes. U.S. government employees, including President Donald Trump, use many of the same products and internet services purportedly compromised by the tools.

The documents describe CIA efforts—cooperating with friendly foreign governments and the U.S. National Security Agency—to subvert the world's most popular technology platforms, including Apple's iPhones and iPads, Google's Android phones and the Microsoft Windows operating system for desktop computers and laptops.

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

WikiLeaks has a long track record of releasing top secret government documents, and experts who sifted through the material said it appeared legitimate.

Jonathan Liu, a spokesman for the CIA, said: "We do not comment on the authenticity or content of purported intelligence documents." White House spokesman Sean Spicer also declined comment.

Missing from WikiLeaks' trove are the actual hacking tools themselves, some of which were developed by government hackers while others were purchased from outsiders. WikiLeaks said it planned to avoid

distributing tools "until a consensus emerges" on the political nature of the CIA's program and how such software could be analyzed, disarmed and published.

Tuesday's disclosure left anxious consumers who use the products with little recourse, since repairing the software vulnerabilities in ways that might block the tools' effectiveness is the responsibility of leading technology companies. The revelations threatened to upend confidence in an Obama-era government program, the Vulnerability Equities Process, under which federal agencies warn technology companies about weaknesses in their software so they can be quickly fixed.

It was not immediately clear how WikiLeaks obtained the information, and details in the documents could not immediately be verified. WikiLeaks said the material came from "an isolated, high-security network" inside the CIA's Center for Cyber Intelligence but didn't say whether the files were removed by a rogue employee or whether the theft involved hacking a federal contractor working for the CIA or perhaps breaking into a staging server where such information might have been temporarily stored.

"The archive appears to have been circulated among former U.S. government hackers and contractors in an unauthorized manner, one of whom has provided WikiLeaks with portions of the archive," WikiLeaks said in a statement.

Some technology firms on Tuesday said they were evaluating the information. Microsoft Corp. said it was looking into the report, while the maker of secure messaging app Signal said the purported CIA tools affected users' actual phones and not its software design or encryption protocols.

The tools described in the documents carried bizarre names, including

Time Stomper, Fight Club, Jukebox, Bartender, Wild Turkey, Margarita and "RickyBobby," a racecar-driving character in the comedy film, "Talladega Nights."

That RickyBobby tool, the documents said, was intended to plant and harvest files on computers running "newer versions of Microsoft Windows and Windows Server." It operated "as a lightweight implant for target computers" without raising warnings from antivirus or intrusion-detection software. It took advantage of files Microsoft built into Windows since at least 10 years ago.

The files include comments by CIA hackers boasting in slang language of their prowess: "You know we got the dankest Trojans and collection tools," one reads.

The documents show broad exchanges of tools and information among the CIA, NSA and other U.S. intelligence agencies, as well as intelligence services of close allies Australia, Canada, New Zealand and the United Kingdom.

WikiLeaks claimed the CIA used both its Langley, Virginia, headquarters and the U.S. consulate in Frankfurt, Germany, as bases for its covert hackers. The AP found that one purported CIA hack that imitates the Domain Name System—the internet's phone book—traced to an internet domain hosted in Germany.

Jake Williams, a security expert with Augusta, Georgia-based Rendition Infosec who has experience dealing with government hackers, said the files' extensive references to operation security meant they were almost certainly government-backed. "I can't fathom anyone fabricated that amount of operational security concern," he said. "It rings true to me."

In an unusual move, WikiLeaks said it was withholding some secrets

inside the documents. Among them, it said it had withheld details of tens of thousands of "CIA targets and attack machines throughout Latin America, Europe and the United States."

WikiLeaks also said its data included a "substantial library" of digital espionage techniques borrowed from other countries, including Russia.

If the authenticity of the documents is officially confirmed, it would represent yet another catastrophic breach for the U.S. intelligence community at the hands of WikiLeaks and its allies, which have repeatedly humbled Washington with the mass release of classified material, including from the State Department and the Pentagon.

Tuesday's documents purported to be from the CIA's "Embedded Development Branch" discuss techniques for injecting malicious code into computers protected by the personal security products of leading international anti-virus companies. They describe ways to trick anti-virus products from companies including Russia-based Kaspersky Lab, Romania-based BitDefender, Dutch-based AVG Technologies, F-Secure of Finland and Rising Antivirus, a Chinese company.

In the new trove, programmers also posted instructions for how to access user names and passwords in popular internet browsers like Microsoft Internet Explorer, Google Chrome and Mozilla Firefox. Under a list of references in one exchange, users were advised: "Be advised, the following may be low traffic sites, sites in which it might be a good idea to disable JavaScript, etc," referring to a widely used internet programming language. "Remember, practice safe browsing, kidz!" they were told.

Some documents were classified "secret" or "top secret" and not for distribution to foreign nationals. One file said those classifications would protect deployed hacks from being "attributed" to the U.S. government.

The practice of attribution, or identifying who was behind an intrusion, has been difficult for investigators probing sophisticated hacks that likely came from powerful nation-states.

___

Satter reported from Paris. Associated Press writers Stephen Braun, Vivian Salama, Frank Bajak, Tammy Webber and Michael Liedtke contributed to this report.

___

Follow Jack Gillum on Twitter at twitter.com/jackgillum or Raphael Satter at twitter.com/razhael . Both can be reached at www.ap.org/tips .