The New York Times | https://nyti.ms/2mB5Vid

EUROPE

WikiLeaks Releases Trove of Alleged C.I.A. Hacking Documents

Leer en español

By SCOTT SHANE, MATTHEW ROSENBERG and ANDREW W. LEHREN MARCH 7, 2017

WASHINGTON — In what appears to be the largest leak of C.I.A documents in history, WikiLeaks released on Tuesday thousands of pages describing sophisticated software tools and techniques used by the agency to break into smartphones, computers and even Internet-connected televisions.

The documents amount to a detailed, highly technical catalog of tools. They include instructions for compromising a wide range of common computer tools for use in spying: the online calling service Skype; Wi-Fi networks; documents in PDF format; and even commercial antivirus programs of the kind used by millions of people to protect their computers.

A program called Wrecking Crew explains how to crash a targeted computer, and another tells how to steal passwords using the autocomplete function on Internet Explorer. Other programs were called CrunchyLimeSkies, ElderPiggy, AngerQuake and McNugget.

The document dump was the latest coup for the antisecrecy organization and a serious blow to the C.I.A., which uses its hacking abilities to carry out espionage against foreign targets.

The initial release, which WikiLeaks said was only the first installment in a larger collection of secret C.I.A. material, included 7,818 web pages with 943 attachments, many of them partly redacted by WikiLeaks editors to avoid disclosing the actual code for cyberweapons. The entire archive of C.I.A. material consists of several hundred million lines of computer code, the group claimed.

In one revelation that may especially trouble the tech world if confirmed, WikiLeaks said that the C.I.A. and allied intelligence services have managed to compromise both Apple and Android smartphones, allowing their officers to bypass the encryption on popular services such as Signal, WhatsApp and Telegram. According to WikiLeaks, government hackers can penetrate smartphones and collect "audio and message traffic before encryption is applied."

Unlike the National Security Agency documents Edward J. Snowden gave to journalists in 2013 , they do not include examples of how the tools have been used against actual foreign targets. That could limit the damage of the leak to national security. But the breach was highly embarrassing for an agency that depends on secrecy.

Robert M. Chesney, a specialist in national security law at the University of Texas at Austin, likened the C.I.A. trove to National Security Agency hacking tools disclosed last year by a group calling itself the Shadow Brokers.

"If this is true, it says that N.S.A. isn't the only one with an advanced, persistent problem with operational security for these tools," Mr. Chesney said. "We're getting bit time and again."

There was no public confirmation of the authenticity of the documents, which were produced by the C.I.A.'s Center for Cyber Intelligence and are mostly dated from 2013 to 2016. But one government official said the documents were real, and a former intelligence officer said some of the code names for C.I.A. programs, an organization chart and the description of a C.I.A. hacking base appeared to be genuine.

The agency appeared to be taken by surprise by the document dump on Tuesday morning. A C.I.A. spokesman, Dean Boyd, said, "We do not comment on the authenticity or content of purported intelligence documents."

In some regard, the C.I.A. documents confirmed and filled in the details on abilities that have long been suspected in technical circles.

"The people who know a lot about security and hacking assumed that the C.I.A. was at least investing in these capabilities, and if they weren't, then somebody else was — China, Iran, Russia, as well as a lot of other private actors," said Beau Woods, the deputy director of the Cyber Statecraft Initiative at the Atlantic Council in Washington. He said the disclosures may raise concerns in the United States and abroad about “the trustworthiness of technology where cybersecurity can impact human life and public safety.”

There is no evidence that the C.I.A. hacking tools have been used against Americans. But Ben Wizner, the director of the American Civil Liberties Union’s Speech, Privacy, and Technology Project, said the documents suggest that the government has deliberately allowed vulnerabilities in phones and other devices to persist to make spying easier.

“Those vulnerabilities will be exploited not just by our security agencies, but by hackers and governments around the world,” Mr. Wizner said. “Patching security holes immediately, not stockpiling them, is the best way to make everyone’s digital life safer.”

WikiLeaks did not identify the source of the documents, which it called Vault 7, but said they had 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 the source, in a statement, set out policy questions that “urgently need to be debated in public, including whether the C.I.A.’s hacking capabilities exceed its mandated powers and the problem of public oversight of the agency.” The source, the group said, “wishes to initiate a public debate about the security, creation, use, proliferation and democratic control of cyberweapons.”

But James Lewis, an expert on cybersecurity at the Center for Strategic and International Studies in Washington, raised another possibility: that a foreign state, most likely Russia, stole the documents by hacking or other means and delivered them to WikiLeaks, which may not know how they were obtained. Mr. Lewis noted that, according to American intelligence agencies, Russia hacked Democratic targets during the presidential campaign and gave thousands of emails to WikiLeaks for publication.

“I think a foreign power is much more likely the source of these documents than a conscience-stricken C.I.A. whistle-blower,” Mr. Lewis said.

At a time of increasing concern about the privacy of calls and messages, the revelations did not suggest that the C.I.A. can actually break the encryption used by popular messaging apps. Instead, by penetrating the user’s phone, the agency can make the encryption irrelevant by intercepting messages and calls before their content is encrypted, or, on the other end, after messages are decrypted.

WikiLeaks, which has sometimes been accused of recklessly leaking information that could do harm, said it had redacted names and other identifying information from the collection. It said it was not releasing the computer code for actual, usable weapons “until a consensus emerges on the technical and political nature of the C.I.A.’s program and how such ‘weapons’ should be analyzed, disarmed and published.”

The codes names used for projects revealed in the WikiLeaks documents appear to reflect the likely demographic of the cyberexperts employed by the C.I.A. — that is, young and male. There are numerous references to “ Harry Potter,” Pokémon and Adderall, the drug used to treat hyperactivity.

A number of projects were named after whiskey brands. Some were high-end single malt scotches, such as Laphroaig and Ardbeg. Others were from more pedestrian labels, such as Wild Turkey, which was described by its programmers, in mock dictionary style, as “(n.) A animal of the avian variety that has not been domesticated. Also a type of alcohol with a high proof (151).”

Some of the details of the C.I.A. programs might have come from the plot of a spy novel for the cyberage, revealing numerous highly classified — and, in some cases, exotic — hacking programs. One program, code-named Weeping Angel, uses Samsung “smart” televisions as covert listening devices. According to the WikiLeaks news release, even when it appears to be turned off, the television “operates as a bug, recording conversations in the room and sending them over the internet to a covert C.I.A. server.”

The release said the program was developed in cooperation with British intelligence.

If C.I.A. agents did manage to hack the smart TVs, they would not be the only ones. Since their release, internet-connected televisions have been a focus for hackers and cybersecurity experts, many of whom see the sets’ ability to record and transmit conversations as a potentially dangerous vulnerability.

In early 2015, Samsung started to include in the fine print terms of service for its smart TVs a warning that the television sets could capture background conversations. “Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of Voice Recognition,” the warning said.

Another program described in the documents, named Umbrage, is a voluminous library of cyberattack techniques that the C.I.A. has collected from malware produced by other countries, including Russia. According to the WikiLeaks release, the large number of techniques allows the C.I.A. to mask the origin of some of its attacks and confuse forensic investigators.

The WikiLeaks material includes lists of software tools that the C.I.A. uses to create exploits and malware to carrying out hacking. Many of the tools are those used by developers around the world: coding languages, such as Python, and tools like Sublime Text, a program used to write code, and Git, a tool that helps developers collaborate.

But the agency also appears to rely on software designed specifically for spies, such as Ghidra, which in one of the documents is described as “a reverse engineering environment created by the N.S.A.”

The Vault 7 release marks the latest in a series of huge leaks that have changed the landscape for government and corporate secrecy.

In scale, the Vault 7 archive appears to fall into the same category as the biggest leaks of classified information in recent years, including the quarter-million diplomatic cables taken by Chelsea Manning, the former Army intelligence analyst, and given to WikiLeaks in 2010 , and the hundreds of thousands of National Security Agency documents taken by Mr. Snowden in 2013.

In the business world, the so-called Panama Papers and several other large-volume leaks have laid bare the details of secret offshore companies used by wealthy and corrupt people to hide their assets.

Both government and corporate leaks have been made possible by the ease of downloading, storing and transferring millions of documents in seconds or minutes, a sea change from the use of slow photocopying for some earlier leaks, including the Pentagon Papers in 1971.

Follow Matthew Rosenberg on Twitter at @AllMattNYT

Scott Shane and Matthew Rosenberg reported from Washington, and Andrew W. Lehren from New York. Mark Mazzetti contributed reporting.

Get politics and Washington news updates via Facebook, Twitter and in the Morning Briefing newsletter.

A version of this article appears in print on March 8, 2017, on Page A1 of the New York edition with the headline: Documents Said to Reveal Hacking Secrets of C.I.A.