What the CIA thinks of your anti-virus program

March 8 2017, by Raphael Satter

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)

Peppering the 8,000 pages of purported Central Intelligence Agency hacking data released Tuesday by WikiLeaks are reviews of some of the world's most popular anti-virus products.

The hackers are quoted taking potshots at anti-virus firms, suggesting the American intelligence agencies are keenly aware of flaws in the products meant to be keeping us all safe online.

The data published by WikiLeaks isn't systematic enough to draw firm conclusions about the reliability of one product or another and the uncertain dating means the CIA's critiques provide more of a snapshot than an overview.

Still, the posts show America's top cyberspies aren't always flattering about commonly used security software.

COMODO

The CIA appears to give mixed praise to the anti-virus solution by Comodo, the self-described "global leader in cyber security solutions."

One post by an apparent CIA hacker published by WikiLeaks said Comodo is "a colossal pain in the posterior. It literally catches everything until you tell it not to."

Just don't upgrade to Comodo 6.

That version "doesn't catch nearly as much stuff," the hacker appears to say, describing a particularly glaring vulnerability as a "Gaping Hole of DOOM."

Melih Abdulhayoglu, Comodo's chief executive, emphasized the first part of the post, saying that being called a pain by the CIA was "a badge

of honor we will wear proudly." In a statement, he said that the vulnerability described by the CIA was obsolete. Comodo 6 was released in 2013; Comodo 10 was released in January.

KASPERSKY LAB

This is one of the world's leading providers of security protection. But it may not keep you safe from the CIA.

A flaw in the code "enables us to bypass Kaspersky's protections," according to another post .

Founder Eugene Kaspersky dismissed the comment, saying in a Twitter message that the flaw identified in the CIA leak was fixed "years ago."

A statement from his company said a second flaw apparently identified by the agency was fixed in December 2015.

AVIRA

A CIA hacker appears to say that this German-engineered anti-virus product is "typically easy to evade."

The firm said in a statement that it had fixed what it described as "a minor vulnerability" within a few hours of the WikiLeaks release.

It added that it had no evidence that any of its users had been affected by the bug.

AVG

The CIA apparently had a trick to defeat AVG that was "totally sweet." The Netherlands-based Avast, AVG's owner, said it was preparing a

statement on the disclosure.

F-SECURE

One CIA hacker appeared to be particularly scathing about this Finnish firm's security software. It's a "lower tier product that causes us minimal difficulty," one apparent hacker said .

F-Secure noted that the company was described elsewhere , along with Avira, as an "annoying troublemaker." It said there was a broader point to be made about the CIA's apparent decision not to warn anti-virus companies about the flaws in their products.

The agency "considered it more important to keep everybody unsecure ... and maybe use the vulnerability for its own purposes or counter terrorism purposes," F-Secure's chief research officer Mikko Hypponen said in a statement.

BITDEFENDER

The posts aren't complete enough to say for sure, but Bitdefender, a Romanian anti-virus product, seemed to cause CIA hackers a lot of trouble.

One post appears to suggest that Bitdefender could be defeated by a bit of tinkering.

Or maybe not.

"Alas, we've just tried this," a response to the post said. "Bitdefender is still mad."

Bitdefender representative Marius Buterchi said the only conclusion to

draw was that "we are detecting the CIA tools."