

Did NSA plant spyware in computers around world? (Update)

February 18 2015, by Brandon Bailey



This Oct. 8, 2009 file photo, shows a network cable, taken on Oct. 8, 2009, in Duesseldorf, Germany. A new report from Russian cybersecurity firm Kaspersky Lab released Monday, Feb. 16, 2015 said its researchers identified malicious programs or worms that infected computers in multiple countries. Targets appeared to be specifically selected and included military, Islamic activists, energy companies and other businesses, as well as government personnel. (AP Photo/Frank Augstein, File)

Did the National Security Agency plant spyware deep in the hard drives of thousands of computers used by foreign governments, banks and other surveillance targets around the world?

A new report from Russian cybersecurity firm Kaspersky Lab said its researchers identified a new family of malicious programs or worms that infected computers in multiple countries, primarily overseas. Targets appeared to be specifically selected and included military, Islamic activists, energy companies and other businesses, as well as government personnel.

Without naming the United States as the source of the malware, the report said one of the programs has elements in common with the so-called Stuxnet worm, which the New York Times and Washington Post have said was developed by the U.S. and Israeli governments to disrupt Iranian nuclear facilities. Based on their similarities, the creators of both programs "are either the same or working closely together," Kaspersky's report said.

The malware was not designed for financial gain but to collect information through "pure cyberespionage," added Kaspersky researcher Vitaly Kamluk. In its report, the firm said the malware was extremely sophisticated and "expensive to develop."

NSA spokeswoman Vanee Vines declined comment Tuesday, but cited a 2014 presidential directive that instructed U.S. intelligence agencies to respect Americans' privacy while continuing to conduct overseas operations necessary to guard against terrorism or other threats.

Kaspersky researchers said some of the spyware was designed to burrow into the essential software that comes pre-installed on a computer's disk drive, known as firmware. Once there, it was difficult to detect and virtually impossible to remove, and it could gain access to vital codes,

such as the keys to deciphering encrypted files. Kamluk said compromising firmware is a difficult technical challenge that likely requires knowledge of the manufacturer's source code—normally a closely guarded secret.

The report named several disk drive manufacturers whose products were compromised, including Seagate Technology, Western Digital Corp., Toshiba and IBM Corp. While some did not immediately respond to requests for comment, three companies said the report came as news to them.

"We take such threats very seriously," Western Digital spokesman Steve Shattuck said Tuesday, adding in a statement that the company is "in the process of reviewing the report from Kaspersky Labs."

Seagate Technology said it "has no specific knowledge of any allegations regarding third parties accessing our drives." The company said in a statement it's committed to security and takes steps to prevent tampering or "reverse engineering" of its products. Toshiba said it had no knowledge of the malware and declined further comment.

While some of the malware was transmitted over the Internet, Kaspersky said one worm spread through infected USB thumb drives, allowing it to collect information from computers that are "air-gapped" or disconnected from the Internet. Air-gapping is a security practice used at nuclear plants and other sensitive facilities.

Kaspersky also said it uncovered "classic spying methods" in which scientists who attended an international conference in Houston were later sent a CD of conference materials from the event's sponsor. The sponsor apparently didn't know that the disc also contained malware which spread into certain attendees' computers, the researchers said.

Kaspersky said it found signs the malware infected computers in more than 30 countries, with the heaviest concentrations in Iran, Russia, Pakistan, Afghanistan and China. There were relatively few targets in the U.S. and Britain, said Kamluk, who characterized them as individuals living or visiting in those countries rather than companies or institutions based there.

Though it's less well-known in the United States, Kaspersky is respected in the cybersecurity industry and its reports are generally viewed as reputable. While some critics have suggested the firm has close ties to Russian authorities, several experts said Tuesday that it's plausible the United States is behind the [malware](#) identified in the report.

"A lot of nation-states are involved in these activities. Russia, China and the U.S. are in a great cyberarms race," said David DeWalt, chief executive of the Silicon Valley cybersecurity firm FireEye. He noted that China has been implicated in attempts to steal source code and other information from U.S. companies, for example, while Russian authorities have been linked to some hacking efforts.

Some warned that U.S. efforts could have unintended consequences: Foreign customers could become more leery of U.S. tech products if they're suspected of being used for spying. And other hackers may be able to exploit the same vulnerabilities, said cybersecurity expert and author Bruce Schneier.

© 2015 The Associated Press. All rights reserved.

Citation: Did NSA plant spyware in computers around world? (Update) (2015, February 18) retrieved 13 March 2024 from <https://phys.org/news/2015-02-nsa-spyware-world.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is

provided for information purposes only.