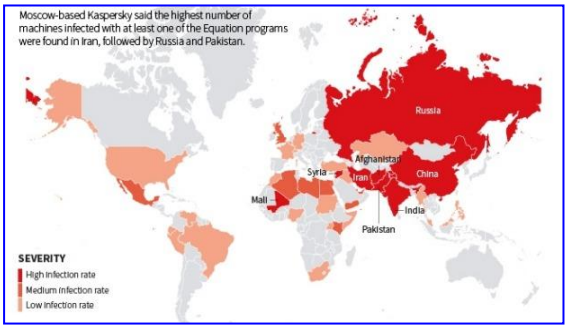
NSA Hiding Equation Spy Program on Hard Drives

Joseph Menn
February 17 2015



Equation infection: Kaspersky Labs says the highest number of machines infected with Equation programs were in Iran, Russia and Pakistan.

The US National Security Agency has figured out how to hide spying software deep within hard drives made by Western Digital, Seagate, Toshiba and other top manufacturers, giving the agency the means to eavesdrop on the majority of the world's computers, according to cyber researchers and former operatives.

That long-sought and closely guarded ability was part of a cluster of spying programs **discovered by Kaspersky Lab**, the Moscow-based security software maker that has exposed a series of Western cyberespionage operations.

Kaspersky said it found personal computers in 30 countries infected with one or more of the spying programs, with the most infections seen in Iran, followed by Russia, Pakistan, Afghanistan, China, Mali, Syria, Yemen and Algeria. The targets included government and military institutions, telecommunication companies, banks, energy companies, nuclear researchers, media, and Islamic activists, Kaspersky said.

The firm declined to publicly name the country behind the spying campaign, but said it was closely linked to Stuxnet, the NSA-led cyberweapon that was used to attack Iran's uranium enrichment facility. The NSA is the agency responsible for gathering electronic intelligence on behalf of the United States.

A former NSA employee told Reuters that Kaspersky's analysis was correct, and that people still in the intelligence agency valued these spying programs as highly as Stuxnet. Another former intelligence operative confirmed that the NSA had developed the prized technique of concealing spyware in hard drives, but said he did not know which spy efforts relied on it. NSA spokeswoman Vanee Vines declined to comment.

Kaspersky published the technical details of its research on Monday, which should help infected institutions detect the spying programs, some of which trace back as far as 2001.

The disclosure could further hurt the NSA's surveillance abilities, already damaged by massive leaks by former contractor Edward Snowden. Snowden's revelations have hurt the United States' relations with some allies and slowed the sales of US technology products abroad.

The exposure of these new spying tools could lead to greater backlash against Western technology, particularly in countries such as China, which is already drafting regulations that would require most bank technology suppliers to proffer copies of their software code for inspection.

TECHNOLOGICAL BREAKTHROUGH. According to Kaspersky, the spies made a technological breakthrough by figuring out how to lodge malicious software in the obscure code called firmware that launches every time…

> *To read this article in its entirety, go to: http://www.stuff.co.nz/technology/digital-living/66279485/nsa-hiding-equation-spy-program-on-hard-drives*