The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

Russia's Kaspersky Lab Exposes U.S. Cyber Espionage Program

By The Moscow Times

February 17, 2015

Kaspersky Lab said it found personal computers in 30 countries infected with one or more of the U.S. spying programs.

SAN FRANCISCO / MOSCOW — Russia's intelligence services are not concerned by the discovery of an advanced cyber-espionage ring discovered by the Moscow-based security software maker Kaspersky Lab, state news agency RIA Novosti reported Tuesday, citing an intelligence official.

Cyber researchers and former operatives said Monday that the cluster of spying programs discovered by Kaspersky Lab shows that the U.S. 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.

“Our computer network is protected against such attacks,” Sergei Ivanov, a representative of

Russia's Foreign Intelligence Service (SVR), told RIA Novosti.

An unidentified representative of Russia's domestic intelligence arm, the Federal Security Service (FSB), echoed the SVR's confidence in their ability to defend against the increasingly sophisticated threat from cyber attacks.

“The FSB's network has reliable protection against hackers,” the representative was cited by RIA as saying.

Kaspersky, which has previously exposed a series of Western cyber espionage operations, 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 U.S. agency responsible for gathering electronic intelligence.

A former NSA employee said Kaspersky's analysis was correct, and that people still in the spy agency valued these espionage 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 said the agency was aware of the Kaspersky report but would not comment on it publicly.

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

The disclosure could hurt the NSA's surveillance abilities, already damaged by massive leaks by former contractor Edward Snowden. Snowden's revelations have upset some U.S. allies and slowed the sales of U.S. 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.

Peter Swire, one of five members of U.S. President Barack Obama's Review Group on Intelligence and Communications Technology, said the Kaspersky report showed that it is essential for the country to consider the possible impact on trade and diplomatic relations before deciding to use its knowledge of software flaws for intelligence gathering.

"There can be serious negative effects on other U.S. interests," Swire said.

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 a computer is turned on.

Disk drive firmware is viewed by spies and cybersecurity experts as the second most valuable real estate on a PC for a hacker, second only to the BIOS code invoked automatically as a computer boots up.

"The hardware will be able to infect the computer over and over," lead Kaspersky researcher Costin Raiu said in an interview.

Though the leaders of the still-active espionage campaign could have taken control of thousands of PCs, giving them the ability to steal files or eavesdrop on anything they wanted, the spies were selective and only established full remote control over machines belonging to the most desirable foreign targets, according to Raiu. He said Kaspersky found only a few especially high-value computers with the hard-drive infections.

Kaspersky's reconstructions of the spying programs show that they could work in disk drives sold by more than a dozen companies, comprising essentially the entire market. They include Western Digital Corp, Seagate Technology Plc, Toshiba Corp, IBM, Micron Technology Inc and Samsung Electronics Co Ltd.

Western Digital, Seagate and Micron said they had no knowledge of these spying programs. Toshiba and Samsung declined to comment. IBM did not respond to requests for comment.

Getting the Source Code

Raiu said the authors of the spying programs must have had access to the proprietary source code that directs the actions of the hard drives. That code can serve as a roadmap to vulnerabilities, allowing those who study it to launch attacks much more easily.

"There is zero chance that someone could rewrite the [hard drive] operating system using public information," Raiu said.

Concerns about access to source code flared after a series of high-profile cyberattacks on Google Inc. and other U.S. companies in 2009 that were blamed on China. Investigators have said they found evidence that the hackers gained access to source code from several big U.S. tech and defense companies.

It is not clear how the NSA may have obtained the hard drives' source code. Western Digital spokesman Steve Shattuck said the company "has not provided its source code to government agencies." The other hard drive makers would not say if they had shared their source code with the NSA.

Seagate spokesman Clive Over said it has "secure measures to prevent tampering or reverse engineering of its firmware and other technologies." Micron spokesman Daniel Francisco said the company took the security of its products seriously and "we are not aware of any instances of foreign code."

According to former intelligence operatives, the NSA has multiple ways of obtaining source code from tech companies, including asking directly and posing as a software developer. If a company wants to sell products to the Pentagon or another sensitive U.S. agency, the government can request a security audit to make sure the source code is safe.

"They don't admit it, but they do say, 'We're going to do an evaluation, we need the source code,'" said Vincent Liu, a partner at security consulting firm Bishop Fox and former NSA analyst. "It's usually the NSA doing the evaluation, and it's a pretty small leap to say they're going to keep that source code."

The NSA declined to comment on any allegations in the Kaspersky report. Vines said the agency complies with the law and White House directives to protect the U.S. and its allies "from a wide array of serious threats."

Kaspersky called the authors of the spying program "the Equation group," named after their embrace of complex encryption formulas.

The group used a variety of means to spread other spying programs, such as by compromising jihadist websites, infecting USB sticks and CDs, and developing a self-spreading computer worm called Fanny, Kaspersky said.

Fanny was like Stuxnet in that it exploited two of the same undisclosed software flaws, known as "zero days," which strongly suggested collaboration by the authors, Raiu said. He added that it was "quite possible" that the Equation group used Fanny to scout out targets for Stuxnet in Iran and spread the virus.

(Reuters, MT)

Original url:
https://www.themoscowtimes.com/2015/02/17/russias-kaspersky-lab-exposes-us-cyber-espionage-program-a43949