TECHNOLOGY NEWS | Thu Sep 22, 2016 | 10:44pm EDT

Exclusive: Probe of leaked U.S. NSA hacking tools examines operative's 'mistake'

The logo of the U.S. National Security Agency is seen during a visit by U.S. President George W. Bush to the agency's installation in Fort Meade, Maryland, January 25, 2006. Bush met with workers and made remarks on American national security at the high-security... REUTERS/Jason Reed - RTR18ZAD

TRENDING STORIES

1 Hurricane Matthew kills 26 in Caribbean on destructive path to U.S.

2 Exclusive: Yahoo secretly scanned customer emails for U.S. intelligence - sources

3 Trump backs off praise of Russia's Putin after debate

4 Chicago latest to sanction Wells Fargo for defrauding customers

5 Russia suspends nuclear agreement, ends uranium research pact with United States

By Joseph Menn and John Walcott | SAN FRANCISCO/WASHINGTON

A U.S. investigation into a leak of hacking tools used by the National Security Agency is focusing on a theory that one of its operatives carelessly left them available on a remote computer and Russian hackers found them, four people with direct knowledge of the probe told Reuters.

The tools, which enable hackers to exploit software flaws in computer and communications systems from vendors such as Cisco Systems and Fortinet Inc, were dumped onto public websites last month by a group calling itself Shadow Brokers.

The public release of the tools coincided with U.S. officials saying they had concluded that Russia or its proxies were responsible for hacking political party organizations in the run-up to the Nov. 8 presidential election. On Thursday, lawmakers accused Russia of being responsible.

Various explanations have been floated by officials in Washington as to how the tools were stolen. Some feared it was the work of a leaker similar to former agency contractor Edward Snowden, while others suspected the Russians might have hacked into NSA headquarters in Fort Meade, Maryland.

But officials heading the FBI-led investigation now discount both of those scenarios, the people said in separate interviews.

NSA officials have told investigators that an employee or contractor made the mistake about three years ago during an operation that used the tools, the people said.

That person acknowledged the error shortly afterward, they said. But the NSA did not inform the companies of the danger when it first discovered the exposure of the tools, the sources said. Since the public release of the tools, the companies involved have issued patches in the systems to protect them.

PICTURES

Investigators have not ruled out the possibility that the former NSA person, who has since departed the agency for other reasons, left the tools exposed deliberately. Another possibility, two of the sources said, is that more than one person at the headquarters or a remote location made similar mistakes or compounded each other's missteps.

Representatives of the NSA, the Federal Bureau of Investigation and the office of the Director of National Intelligence all declined to comment.

After the discovery, the NSA tuned its sensors to detect use of any of the tools by other parties, especially foreign adversaries with strong cyber espionage operations, such as China and Russia.

That could have helped identify rival powers' hacking targets, potentially leading them to be defended better. It might also have allowed U.S officials to see deeper into rival hacking operations while enabling the NSA itself to continue using the tools for its own operations.

Because the sensors did not detect foreign spies or criminals using the tools on U.S. or allied targets, the NSA did not feel obligated to immediately warn the U.S. manufacturers, an official and one other person familiar with the matter said.

In this case, as in more commonplace discoveries of security flaws, U.S. officials weigh what intelligence they could gather by keeping the flaws secret against the risk to U.S. companies and individuals if adversaries find the same flaws.

Critics of the Obama administration's policies for making those decisions have cited the Shadow Brokers dump as evidence that the balance has tipped too far toward intelligence gathering.

ALSO IN TECHNOLOGY NEWS

Exclusive: Twitter to conclude sale deliberations this month - sources

Wal-Mart's next move against Amazon: More warehouses, faster shipping

The investigators have not determined conclusively that the Shadow Brokers group is affiliated with the Russian government, but that is the presumption, said one of the people familiar with the probe and a fifth person.

One reason for suspecting government instead of criminal involvement, officials said, is that the hackers revealed the NSA tools rather than immediately selling them.

The publication of the code, on the heels of leaks of emails by Democratic Party officials and preceding leaks of emails by former U.S. Secretary of State Colin Powell, could be part of a pattern of spreading harmful and occasionally false information to further the Russian agenda, said Jim Lewis, a cybersecurity expert at the Center for Strategic and International Studies.

"The dumping is a tactic they've been developing for the last five years or so," Lewis said. "They try it, and if we don't respond they go a little further next time."

(Reporting by Joseph Menn in San Francisco and John Walcott in Washington; Editing by Jonathan Weber and Grant McCool)

NEXT IN TECHNOLOGY NEWS

Replacement Samsung Note 7 phone emits smoke on U.S. plane: family

LOUISVILLE, Ky. A replacement model of the fire-prone Samsung Note 7 smartphone began smoking inside a U.S. plane on Wednesday, the family that owns it said, prompting fresh investigations by the Consumer Product Safety Commission and the Federal Aviation Administration.

Dialog Semi reviews guidance as Chinese holiday boosts third quarter sales

FRANKFURT Dialog Semiconductor , the maker of chips used in Apple and Samsung Electronics' smartphones, said it was reviewing its full-year guidance after a Chinese holiday helped bolster third-quarter sales.

Pictures of the day

SPONSORED TOPICS