U.S. intelligence agencies say Russia likely behind hacking of government agencies

SAN FRANCISCO (Reuters) -The office of the U.S. Director of National Intelligence on Tuesday said Russia was “likely” behind a string of hacks identified last month that gained access to several federal agencies.

The office, along with the FBI, the National Security Agency, and Cybersecurity and Infrastructure Security Agency inside the Department of Homeland Security, in a joint statement, said the hackers’ goal appeared to be collecting intelligence, rather than any destructive acts. They said they had so far identified “fewer than 10” agencies that were hacked.

The agencies said that the actor, “likely Russian in origin, was responsible for most or all of the recently discovered, ongoing cyber compromises of both government and non-governmental networks.” The investigation is continuing, they said and could turn up additional government victims.

It was the first formal statement of attribution by the Trump administration.

Elected officials briefed on the inquiry and Secretary of State Mike Pompeo had previously said Russia was behind the hacking spree, but President Donald Trump said it could have been China.

The incoming administration of Joe Biden has already promised a response to the SolarWinds hacks. On Tuesday, the top Democrats on the Congressional intelligence committees underscored that need.

“Congress will need to conduct a comprehensive review of the circumstances leading to this compromise, assess the deficiencies in our defenses, take stock of the sufficiency of our response in order to prevent this from happening again, and ensure that we respond appropriately,” said Rep. Adam Schiff, head of the House committee.

Russian officials have denied involvement and did not immediately respond to questions Tuesday.

The penetration of departments including Defense, State, Homeland Security, Treasury, and Commerce is already considered the worst known cyber-compromise at least since electronic dossiers on most Americans with security clearances were taken from the Office of Personnel Management five years ago.

Officials briefed on the case said that the main target of the hackers appeared to be email. One said that no classified networks seem to have been breached and that fewer than 50 private companies had been fully compromised, a lower number than initially feared.

The security company FireEye Inc, which was itself breached, discovered the new round of attacks, many of which were traced to a tainted software update from SolarWinds Corp, which makes widely used network-management programs.

It remains unknown how the hackers got deep inside SolarWinds' production system as long as a year ago. Once there, they were able to slip "back doors" into two digitally signed updates of the company's flagship Orion software.

As many as 18,000 customers downloaded those updates, which sent signals back to the hackers. At a small number of high-value targets, the group then manipulated access to cloud services in order to read emails or other content and potentially installed other back doors, making clean-up after discovery a daunting task.

A few major technology companies have said they had at least downloaded the bad code from SolarWinds, and Microsoft Corp said Dec. 31 that the penetration had gone well beyond that, allowing the intruders to view its prized source code, where they might have looked for security flaws. here

The attackers also hacked sellers of Microsoft services, which often maintain access to customers, to go after email at non-SolarWinds customers, according to security company CrowdStrike Holdings Inc and Microsoft employees.

Microsoft and federal investigators have not said how many resellers were hacked or how many customers were impacted.

The overall strategy of electronic infiltration through vendors, known as a supply-chain attack, is especially effective, and officials fear the success of the current wave will encourage more of them.

Reporting by Joseph Menn and Chris Bing; Additional reporting by Raphael Satter and Mark Hosenball; Editing by Leslie Adler, Alistair Bell, and Christopher Cushing

Our Standards: The Thomson Reuters Trust Principles.

Source:
https://www.reuters.com/article/us-global-cyber/u-s-intelligence-agencies-say-russia-likely-behind-hacking-of-government-agencies-idUSKBN29A2HG

[Disclaimer]