The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

Pompeo Blames Russia for Massive U.S. Cyberattack

By Rob Lever for AFP

December 19, 2020

U.S. Secretary of State Mike Pompeo **AP**

Russia was "pretty clearly" behind a devastating cyberattack on several U.S. government agencies that also hit targets worldwide, Secretary of State Mike Pompeo said.

Microsoft said late Thursday that it had notified more than 40 customers hit by the malware, which security experts say could allow attackers unfettered network access to key government systems and electric power grids and other utilities.

"There was a significant effort to use a piece of third-party software to essentially embed code inside of U.S. government systems," Pompeo told The Mark Levin Show on Friday.

"This was a very significant effort, and I think it's the case that now we can say pretty clearly that it was the Russians that engaged in this activity."

Roughly 80 percent of the affected customers are located in the United States, Microsoft

president Brad Smith said in a blog post, with victims also found in Belgium, Britain, Canada, Israel, Mexico, Spain and the United Arab Emirates.

"It's certain that the number and location of victims will keep growing," Smith said, echoing concerns voiced this week by U.S. officials on the serious threat from the attack.

"This is not 'espionage as usual,' even in the digital age," Smith said.

"Instead, it represents an act of recklessness that created a serious technological vulnerability for the United States and the world."

John Dickson of the security firm Denim Group said many private sector companies which could be vulnerable were scrambling to shore up security, even to the point of considering rebuilding servers and other equipment.

"Everyone is in damage assessment now because it's so big," Dickson said. "It's a severe body blow to confidence both in government and critical infrastructure."

The threat comes from a long-running attack which is believed to have injected malware into computer networks using enterprise management network software made by the Texas-based IT company SolarWinds, with the hallmarks of a nation-state attack.

James Lewis, vice president at the Center for Strategic and International Studies, said the attack may end up being the worst to hit the United States, eclipsing the 2014 hack of US government personnel records in a suspected Chinese infiltration.

"The scale is daunting. We don't know what has been taken so that is one of the tasks for forensics," Lewis said.

"We also don't know what's been left behind. The normal practice is to leave something behind so they can get back in, in the future."

Related article: U.S. Government Confirms Cyberattack After Reports of Russia-Linked Hacking

- NSA warning -

The National Security Agency called for increased vigilance to prevent unauthorized access to key military and civilian systems.

Analysts have said the attacks pose threats to national security by infiltrating key government systems, while also creating risks for controls of key infrastructure systems such as electric power grids and other utilities.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) said government agencies, critical infrastructure entities, and private sector organizations had been targeted by what it called an "advanced persistent threat actor."

CISA did not identify who was behind the malware attack, but private security companies

pointed a finger at hackers linked to the Russian government.

Pompeo had also suggested Moscow's involvement on Monday, saying the Russian government had made repeated attempts to breach U.S. government networks.

President-elect Joe Biden expressed "great concern" over the computer breach while Republican Senator Mitt Romney blamed Russia and slammed what he called "inexcusable silence" from the White House.

Romney likened the cyberattack to a situation in which "Russian bombers have been repeatedly flying undetected over our entire country."

CISA said the computer intrusions began at least as early as March this year, and the actor behind them had "demonstrated patience, operational security and complex tradecraft."

"This threat poses a grave risk," CISA said Thursday, adding that it "expects that removing this threat actor from compromised environments will be highly complex and challenging for organizations."

Hackers reportedly installed malware on software used by the U.S. Treasury Department and the Commerce Department, allowing them to view internal email traffic.

The Department of Energy, which manages the country's nuclear arsenal, confirmed it had also been hit by the malware but had disconnected affected systems from its network.

"At this point, the investigation has found that the malware has been isolated to business networks only, and has not impacted the mission essential national security functions of the department, including the National Nuclear Security Administration," said agency spokeswoman Shaylyn Hynes.

SolarWinds said up to 18,000 customers, including government agencies and Fortune 500 companies, had downloaded compromised software updates, allowing hackers to spy on email exchanges.

Russia has denied involvement.

Original url:
https://www.themoscowtimes.com/2020/12/19/pompeo-blames-russia-for-massive-us-cyberattack-a72412