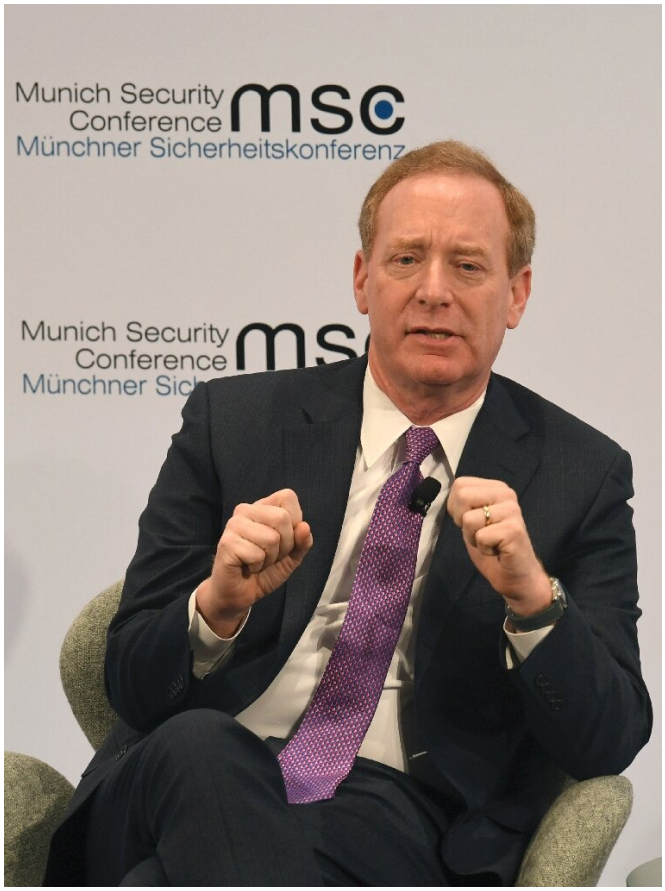
Massive cyberattack grows beyond US, heightening fears

18 December 2020, by Rob Lever



Microsoft president Brad Smith said the massive cyberattack is more than "espionage as usual" and represents a major threat to the US and the world

A devastating cyberattack on US government agencies has also hit targets worldwide, with the list of victims still growing, according to researchers, heightening fears over computer security and espionage.

Microsoft said late Thursday that it had notified more than 40 customers hit by the malware, which security experts say came from hackers linked to the Russian government and which could allow attackers unfettered network access.

"While roughly 80 percent of these customers are located in the United States, this work so far has also identified victims in seven additional countries," Microsoft president Brad Smith said in a blog post.

Smith said the victims were 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 US 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 firms which could be vulnerable are scrambling to shore up security, even to the point of considering rebuilding their 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."

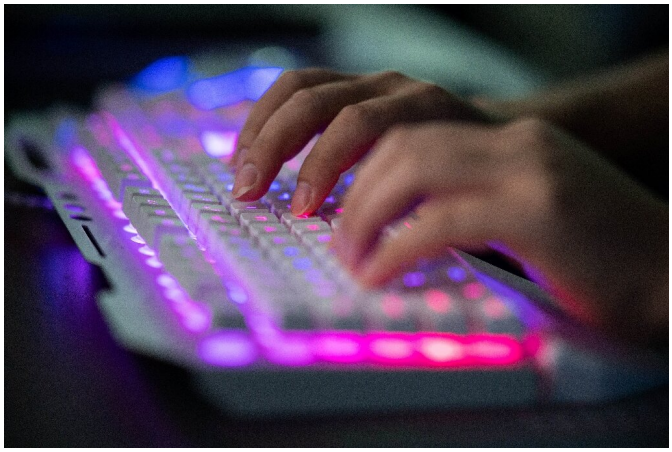
The threat comes from a long-running attack which is believed to have injected malware into computer networks using enterprise management network software made by the Texas-based IT company SolarWinds, with the hallmarks of a nation-state attack.

James Lewis, vice president at the Center for Strategic and International Studies, said the attack may end up being the worst to hit the US, 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."



Investigators and researchers are still learning of the scope of the cyberattack which has hit US government agencies and other victims around the world

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 US 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.

US Secretary of State Mike Pompeo also suggested involvement by Moscow on Monday, saying the Russian government had made repeated attempts to breach US 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."

Senator Marco Rubio, also a Republican, told Fox News: "It is massive. It is still, I would argue, probably persistent. It is still ongoing... It's a grave risk to federal, to state, to local governments, to critical infrastructure, to the private sector."

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 US Treasury Department and the Commerce Department, allowing them to view internal email traffic.

Media reports said the Department of Energy, which manages the government's nuclear arsenal, had also been breached.

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.

After the attack was detected, CISA ordered federal agencies to power down the breached software.