US 'Has Evidence Russia Breached Its Nuclear Networks' in Massive Cyber Attack
2020-12-17 22:16:25.333 GMT

By Matthew Field

(Telegraph) -- The US nuclear weapons agency was hacked as part of a suspected Russian cyber-attack that struck several federal government agencies, it emerged on Thursday.

The Energy Department and the National Nuclear Security Administration have warned Congress that networks they control were breached, including at the Los Alamos National Laboratory, which conducts the government's most sensitive and advanced nuclear research, Politico reported.

Evidence of the attack was also found in the networks of the Federal Energy Regulatory Commission, known as FERC, and the Office of Secure Transportation which is responsible for moving nuclear materials.

The suspected Kremlin hackers are believed to have gained access to networks by installing malicious code in a widely used software program from SolarWinds Corp.

While President Donald Trump has yet to publicly address the hack, President-elect Joe Biden issued a statement Thursday on “what appears to be a massive cybersecurity breach affecting potentially thousands of victims, including US companies and federal government entities.” “I want to be clear," Mr Biden wrote.

"My administration will make cybersecurity a top priority at every level of government -- and we will make dealing with this breach a top priority from the moment we take office.”

Federal investigators have been combing through networks in recent days to determine what hackers had been able to access and how much damage might have done in one of the most serious cyber attacks on the US government in recent years.

Thomas Bossert, Mr Trump's former homeland security adviser, warned that a Russian cyber attack on the US government could take more than six months to resolve and will require a “staggering effort” to rebuild existing IT systems.

As the sweeping scale of the attack - which began in March - continues to

emerge, US intelligence agencies have ordered departments to “disconnect or power down” all equipment from SolarWinds, a hacked Texas-based provider of network management software.

Its Orion software, which is widely used by thousands of government agencies and companies around the world, is thought to have been exploited by Russian attackers in a highly sophisticated cyber attack. It went undetected for nine months, offering access to computer networks, emails and other data.

The US State Department, Treasury and Commerce Department, Homeland Security and parts of the Pentagon are all said to have been affected.

US government departments remain highly vulnerable because its lengthy duration may have allowed attackers to burrow deep inside networks using new methods, potentially thwarting counter-espionage efforts now underway.

Solar Winds' Orion software is used to manage and secure company and government networks. It is used by multiple US agencies and UK departments including GCHQ. The National Cyber Security Centre (NCSC) is investigating any possible UK impact.

The NCSC has advised victims to isolate affected software and apply a security patch.

Alan Woodward, a former GCHQ consultant, cautioned the US plan was a “knee-jerk reaction” and risked creating further problems.

“These systems are so intertwined you can’t rip one bit out and not expect it to impact another,” he said. “It has tendrils in everything.” He confirmed a timeline of up to six months was possible for a full rebuild.

The incident of cyber espionage has been described as the most damaging hack of 2020, with the US Treasury and Commerce departments spied on for months with emails exposed. Dozens of other agencies are now scrambling to determine if they are also at risk.

In its directive US departments, the US cyber agency said all departments should disconnect Orion products, treat them as “compromised”, and rebuild using “trusted sources”.

Mark Arena, a cyber security expert at Intel 471, said this may not be enough. He said: “This attack could have been going on for over a year. I don’t think it will be enough. What else has happened that we don’t know about yet?”

Senator Richard Blumenthal, a senior Democract senator, formally blamed Russia for the attack adding the “cyberattack left me deeply alarmed, in fact downright scared”. Russia has denied any involvement.

Democratic Senator Dick Durbin said the attack was “virtually a declaration of war” from Russia. However, security experts cautioned against escalation.

-0- Dec/17/2020 22:16 GMT

To view this story in Bloomberg click here:
https://blinks.bloomberg.com/news/stories/QLI8JD3HBS3K

c