US moves closer to retaliation over hacking as cyber woes grow

March 12 2021

Credit: CC0 Public Domain

A senior US official said Friday the Biden administration is close to a decision on retaliation for state-sponsored hacking as fears grew over the fallout from the latest of two major cyberattacks.

The official said the White House was working closely with the private sector to ramp up cyber defenses following the attacks which targeted Microsoft Exchange servers and SolarWinds security software, potentially compromising thousands of government and private computer networks.

US officials had previously hinted at moves against Russia, which has been linked to the massive SolarWinds hack that shook the government and corporate security last year. The latest comments suggested forthcoming actions.

"You can expect further announcements on that in weeks, not months," the senior official said, in reference to SolarWinds, in a briefing with reporters on the two hacking incidents.

The official, who asked not to be identified, said federal agencies had made progress in patching systems at nine federal agencies affected by the SolarWinds attack.

But an urgent effort is underway to remedy the Microsoft Exchange hack, which opened security holes that are actively being exploited by cybercriminals and others.

To help find solutions, "for the first time we've invited private sector companies to participate" in key national security meetings on the attacks, the official said.

The response "is still evolving," according to the official, who noted: "We really have a short window to get vulnerable servers patched, measured in hours, not days."

New ransomware emerges

The comments came as a new strain of ransomware has emerged which exploits a security flaw in Microsoft Exchange servers, signaling potentially damaging consequences from the high-profile hack.

Microsoft and other security researchers said the new ransomware dubbed "DearCry" was showing up in servers affected by the breach attributed to a Chinese hacker group.

"We have detected and are now blocking a new family of ransomware being used after an initial compromise of unpatched on-premises Exchange Servers," said a tweet from Microsoft Security Intelligence.

Other researchers including Michael Gillespie, founder of the ID Ransomware service, noted the new strain of malware on Thursday, which could lead to a new wave of attacks that encrypt computer systems and seek to extract payments from operators.

This is the latest sign that the security flaw which became public this month could open the door to a variety of hackers, cybercriminals and cyberespionage operators.

"While patching to prevent compromises will be easy, remediating any systems that have already been compromised will not," said Brett Callow of the security firm Emsisoft.

"At this point, it's absolutely critical that governments quickly come up with a strategy to help organizations secure their Exchange servers and remediate any compromises before an already bad situation becomes even worse."

Earlier this week the FBI and Department of Homeland Security warned that the Exchange server vulnerability may be exploited for nefarious purposes.

A joint statement by the agencies said that "adversaries could exploit these vulnerabilities to compromise networks, steal information, encrypt data for ransom, or even execute a destructive attack."

The DHS Cybersecurity and Infrastructure Security Agency has been pressing for patches to be applied to networks in both government and the private sector.

The potentially devastating hack is believed to have affected at least 30,000 Microsoft email servers in government and private networks and has prompted calls for a firm response to state-sponsored attacks which could involve "hacking back" or other measures.