Every Computer Network In The USA Has Been Hacked And Anybody Who Does Not Know That Is Going To Suffer

The Cybersecurity and Infrastructure Security Agency (CISA) revealed that the massive global hacking campaign conducted by foreign actors is even larger than originally reported.

The cyber actors gained secretive backdoor access in more ways than just through the publicly known SolarWinds software update being corrupted.

“One of the initial access vectors for this activity is a supply chain compromise of the SolarWinds Orion products. CISA has evidence of additional initial access vectors, other than the SolarWinds Orion platform; however, these are still being investigated,” CISA wrote emphasizing that “**the SolarWinds Orion supply chain compromise is not the only initial infection vector this advanced persistent threat actor leveraged.” In other words: EVERYTHING IS HACKED!**

The federal security agency also warned hat “this threat poses a grave risk to the Federal Government and state, local, tribal, and territorial governments as well as critical infrastructure entities and other private sector organizations.”

CISA said that the foreign hackers had compromised “U.S. government agencies, critical infrastructure entities, and private sector organizations” beginning “at least” in March and that the cyber actors “demonstrated patience, operational security, and complex tradecraft in these intrusions.”

The agency added that it “expects that removing this threat actor from compromised environments will be highly complex and challenging for organizations” and that “it is likely that the adversary has additional initial access vectors and tactics, techniques, and procedures that have not yet been discovered.”

CISA issued a government-wide directive to purge all federal agency networks of potentially compromised servers after discovering that, at the very least, the Treasury and Commerce departments were victims of a months long cyber campaign suspected by many to be a Russian hacking effort. The Department of Homeland Security, the State Department, and the National Institutes of Health are also believed to be victims.

SolarWinds acknowledged Sunday night that its systems had been compromised by hackers who infiltrated the company's Orion software updates in order to distribute malware to its customers' computers. The U.S. network-management company said roughly 18,000 of its customers were affected. Before the customers were removed from the company website, ***it boasted its 300,000 customers included "more than 425 of the US Fortune 500," the 10 biggest telecommunications companies in the United States, "all five branches" of the U.S. military, and a number of different government agencies — including the State Department, the National Security Agency, the Justice Department, and the Office of the President.***

The FBI, CISA, and the Office of the Director of National Intelligence released a joint statement revealing that the “cybersecurity campaign” was “significant and ongoing.” The groups established a Cyber Unified Coordination Group to respond to the crisis and warned that “while we continue to work

to understand the full extent of this campaign, we know this compromise has affected networks within the federal government."

FireEye, a cybersecurity firm that works with government agencies to expose and fight foreign cyberattacks, reported that it discovered a " highly evasive attacker" infiltrated SolarWinds's Orion software updates. The firm announced last week it had itself also been hacked.

A FireEye spokesperson told the *Washington Examiner* on Wednesday that "SUNBURST is the malware that was distributed through SolarWinds software" and that "as part of FireEye's analysis of SUNBURST, we identified a killswitch that would prevent SUNBURST from continuing to operate." The group said that "this killswitch will affect new and previous SUNBURST infections by disabling SUNBURST deployments … however, in the intrusions FireEye has seen, this actor moved quickly to establish additional persistent mechanisms to access to victim networks beyond the SUNBURST backdoor."

Thomas Bossert, a former Trump homeland security adviser, warned in the *New York Times* on Wednesday that "the magnitude of this ongoing attack is hard to overstate." He said that "the Russians have had access to a considerable number of important and sensitive networks for six to nine months" and that "the logical conclusion is that we must act as if the Russian government has control of all the networks it has penetrated."

"We are aware of a potential vulnerability which, if present, is currently believed to be related to updates which were released between March and June 2020 to our Orion monitoring products," Kevin Thompson, the CEO of SolarWinds, told the *Washington Examiner* over the weekend. "We believe that this vulnerability is the result of a highly sophisticated, targeted, and manual supply chain attack by a nation-state."

China, Iran and Russia have ongoing efforts this large. All of the hacking tools they use are freely available on the internet. Any 14 year old can use the tools to hack others. CIA, NSA, DOJ, SSA, NASA and other systems are known to be fully infected. Due to the recent elections, political attack operatives in the USA commonly hack those they wish to seek reprisal against. Every hour, someone is hacked in order to blackmail them!

Just remember: ***more than 425 of the US Fortune 500," the 10 biggest telecommunications companies in the United States, "all five branches" of the U.S. military, and a number of different government agencies — including the State Department, the National Security Agency, the Justice Department, and the Office of the President have all been hacked say CISA and the FBI!***