Struggle-La-Lucha.org

Spies are going to spy. Five questions on the so-called Russian hack

written by Gary Wilson
December 24, 2020

A SolarWinds adviser warned the company that it was an “incredibly easy target to hack.”

“Russian Hackers Broke Into Federal Agencies, U.S. Officials Suspect,” was the Dec. 13 New York Times headline on a report by David Sanger.

U.S. Sen. Dick Durbin said the hack is “virtually a declaration of war.” U.S. Sen. Marco Rubio said that “America must retaliate, and not just with sanctions.” A Reuters headline said, “Biden’s options for Russian hacking punishment: sanctions, cyber retaliation.”

What’s really going on?

1. What is the role of the media?

The report on the hack in the New York Times said that Russia did it, even though none of the agencies reporting the hack cited Russia in any way.

David Sanger’s report said the official story is that Russia hacked into U.S. government networks.

That became the story used by all the big media in the U.S. For example, NBC followed with a report that the U.S. Cybersecurity and Infrastructure Security Agency “has not said who it thinks is the ‘advanced persistent threat actor’ behind the ‘significant and ongoing’ campaign, but many experts are pointing to Russia.”

Sanger has written multiple pieces blaming Russia for hacking, much like what he and his colleague, Judith Miller, did leading up to the U.S. war on Iraq, insisting on the presence of weapons of mass destruction — weapons that never existed.

Sanger was also an originator and promoter of the false claim of a Russian hack of the Democratic National Committee and top officials in the 2016 Hillary Clinton campaign. That accusation was used as a distraction after it was learned that WikiLeaks was about to publish emails that showed how Clinton and the DNC had intervened to block Bernie Sanders.

Too many still believe the Russia hacking and Trump campaign conspiracy story. But, like the weapons of mass destruction, it never happened.

2. What happened?

About 18,000 organizations around the world downloaded a software update for the SolarWinds Orion network management tools that contained a hidden software tool that opened a backdoor into any system running Orion. That was reported by SolarWinds on Dec. 14.

The SolarWinds Orion software is used by nearly all Fortune 500 companies, all of the top 10 telecommunications companies, all five branches of the U.S. military, and all of the top five accounting firms. SolarWinds software is used by more than 300,000 companies and government agencies around the world.

According to Microsoft President Brad Smith, of the 18,000 organizations that downloaded the backdoored app, only 0.02% were actually accessed through the backdoor, that is, only 40 corporations or agencies. Most were in the U.S., but not all.

Of the 40 institutions accessed through a follow-up hack, 44% were tech companies and 18% were government agencies. The rest were other kinds of private companies.

Microsoft's Smith says that this kind of operation is typically done by private cybersecurity companies.

Smith writes: "One illustrative company in this new sector [private cybersecurity companies] is the NSO Group, based in Israel and now involved in U.S. litigation. NSO created and sold to governments an app called Pegasus, which could be installed on a device simply by calling the device via WhatsApp; the device's owner did not even have to answer. According to WhatsApp, NSO used Pegasus to access more than 1,400 mobile devices, including those belonging to journalists and human rights activists."

3. Who did it?

The actual security reports on the attack say no source for the hack can be identified. There is no evidence that Russia was involved. If there was, the media would have presented it instead of attributing the charge to anonymous sources.

The hack was discovered by the network security company FireEye. "The highly evasive attacker" used "difficult-to-attribute tools," FireEye said. Neither FireEye nor Microsoft could identify any source for the "difficult-to-attribute" intrusion.

Max Abrahms, an international security professional and author of a book on terrorism, said on Twitter: "'The U.S. government did not publicly identify Russia as the culprit behind the hacks, first reported by Reuters, and said little about who might be responsible.'

"You know this story will be retold as all 17 intel agencies 100% certain Putin is behind it."

A second Tweet by Abrahms added:

"American Media:

"1. Punish Russia

"2. Possibly continue investigating whether the Russian government carried out the cyberattack

“3. Only report evidence corroborating the media’s priors that Moscow was behind the attack

“4. Find additional rationales to punish Russia.”

4. What was the hack?

The hack was in some ways very simple. The SolarWinds Orion software is used by companies and agencies to centrally monitor IT systems. It provides information on the internal systems being run by the company. It is a system used to monitor network and server performance.

A SolarWinds adviser warned the company that it was an “incredibly easy target to hack.” Ian Thornton-Trump, who now works as the chief information security officer at Cyjax, told Bloomberg News that he’d warned SolarWinds in 2017 of its vulnerability. According to the Bloomberg report, access to the Orion software distribution server that delivers system updates used the password “solarwinds123,” which was publicly visible until sometime in 2019.

The hacking software that was put on the SolarWinds Orion distribution server was newly developed, according to FireEye. It was not built using hacking tools that were developed by the U.S. Defense Department’s National Security Agency (NSA) that were leaked in 2017 and have become the primary tools used for spying operators outside the U.S.

The capability to develop these kinds of spy tools is held primarily by the NSA, along with Britain’s Government Communications Headquarters (GCHQ) and Israel. China and Russia have some capability. Microsoft’s Brad Smith suggests that it is likely a private cybersecurity company that is involved.

Despite the lack of evidence that points to a specific actor, the U.S. media immediately blamed Russia for the spying attempt.

5. Was this an act of war?

Cybersecurity and legal experts say that the hack would not be considered an act of war under international law and most experts consider it a routine act of espionage. Espionage is internationally allowed in peacetime.

To qualify as an act of war, United Nations resolutions and other sources of international law require the use of force or destruction. In this case, there has been no loss of life or damage of any kind to the infrastructure. The hack has been for data collection only. The intrusion has not reached any systems on the specially protected "secret" networks.

The hackers gained access to the U.S. Treasury Department's unclassified systems but really just saw what the system was doing, the applications running and that sort of thing.

"At this point, we do not see any break-in into our classified systems," Treasury Secretary Steve Mnuchin said on CNBC. "Our unclassified systems did have some access. I will say the good is there's been no damage, nor have we seen any large amounts of information displaced."

Breaking into unclassified government and corporate networks, reading other people's emails — that's spying. That's the kind of cyber spying that the National Security Agency does 24 hours a day against Russia, China, Iran, Cuba, Venezuela and many more.

"Warfare implies violence, death and destruction," said Duncan Hollis, a professor of law at Temple University specializing in cybersecurity. Hollis and other experts said the attack appears to have been carried out to steal sensitive U.S. information, and should be viewed as espionage.

“Simply stealing information, as much as we don’t like it, is not an act of war — it is espionage,” said Benjamin Friedman, a policy director at the think tank Defense Priorities.

The U.S. is the primary purveyor of espionage in the world. As Edward Snowden revealed, the U.S. Defense Department’s NSA is engaged in this kind of data collection on a global scale as well as in the U.S.

There is a difference between espionage and war.

Take it from Carl von Clausewitz, the Prussian general and military theorist whose “On War” is required reading at West Point. Clausewitz wouldn’t consider this “war” either, says Tom Mahnken, a veteran of long service in the Navy and civilian Pentagon posts who now heads the Center for Strategic and Budgetary Assessments.

Clausewitz defined war as “an act of force to compel our enemy to do our will,” Mahnken noted. “What remains essential to war is that it is meant to compel an adversary — to achieve political objectives. That’s not what this hack is about: It is a classic intelligence-gathering operation.”

https://www.struggle-la-lucha.org/2020/12/24/spies-are-going-to-spy-five-questions-on-the-so-called-russian-hack/