Hacked networks will need to be burned 'down to the ground'

19 December 2020, by Frank Bajak

This Wednesday, Feb. 11, 2015 file photo shows FireEye offices in Milpitas, Calif. Experts say it's going to take months to kick elite hackers widely believed to be Russian out of U.S. government networks. The hackers have been quietly rifling through those networks for months in Washington's worst cyberespionage failure on record. FireEye is the cybersecurity company that discovered the worst-ever intrusion into U.S. agencies and was among the victims. It has already tallied dozens of casualties. It's racing to identify more. (AP Photo/Ben Margot)

It's going to take months to kick elite hackers widely believed to be Russian out of the U.S. government networks they have been quietly rifling through since as far back as March in Washington's worst cyberespionage failure on record.

Experts say there simply are not enough skilled threat-hunting teams to duly identify all the government and private-sector systems that may have been hacked. FireEye, the cybersecurity company that discovered the intrusion into U.S. agencies and was among the victims, has already tallied dozens of casualties. It's racing to identify more.

"We have a serious problem. We don't know what networks they are in, how deep they are, what access they have, what tools they left," said Bruce Schneier, a prominent security expert and Harvard fellow.

It's not clear exactly what the hackers were seeking, but experts say it could include nuclear secrets, blueprints for advanced weaponry, COVID-19 vaccine-related research and information for dossiers on key government and industry leaders.

Many federal workers—and others in the private sector—must presume that unclassified networks are teeming with spies. Agencies will be more inclined to conduct sensitive government business on Signal, WhatsApp and other encrypted smartphone apps.

"We should buckle up. This will be a long ride," said Dmitri Alperovitch, co-founder and former chief technical officer of the leading cybersecurity firm CrowdStrike. "Cleanup is just phase one."

The only way to be sure a network is clean is "to burn it down to the ground and rebuild it," Schneier said.

Imagine a computer network as a mansion you inhabit, and you are certain a serial killer as been there. "You don't know if he's gone. How do you get work done? You kind of just hope for the best," he said.

Deputy White House press secretary Brian Morgenstern told reporters Friday that national security adviser Robert O'Brien has sometimes been leading multiple daily meetings with the FBI, the Department of Homeland Security and the intelligence community, looking for ways to mitigate the hack.

He would not provide details, "but rest assured we

have the best and brightest working hard on it each and every single day."

The Democratic chairs of four House committees given classified briefings on the hack by the Trump administration issued a statement complaining that they "were left with more questions than answers."

This June 6, 2013 file photo, shows the sign outside the National Security Agency (NSA) campus in Fort Meade, Md.All fingers are pointing to Russia as author of the worst-ever hack of U.S. government agencies. But President Donald Trump, long wary of blaming Moscow for cyberattacks has so far been silent. (AP Photo/Patrick Semansky, File)

"Administration officials were unwilling to share the full scope of the breach and identities of the victims," they said.

Morgenstern said earlier that disclosing such details only helps U.S. adversaries. President Donald Trump has not commented publicly on the matter, but Secretary of State Mike Pompeo said on a conservative talk show Friday, "I think it's the case that now we can say pretty clearly that it was the Russians that engaged in this activity."

What makes this hacking campaign so extraordinary is its scale—18,000 organizations were infected from March to June by malicious code that piggybacked on popular network-management software from an Austin, Texas, company called SolarWinds.

Only a sliver of those infections were activated to allow hackers inside. FireEye says it has identified dozens of examples, all "high-value targets." Microsoft, which has helped respond, says it has identified more than 40 government agencies, think tanks, government contractors, non-governmental organizations and technology companies infiltrated by the hackers, 75% in the United States.

Florida became the first state to acknowledge falling victim to a SolarWinds hack. Officials told The Associated Press on Friday that hackers apparently infiltrated the state's health care administration agency and others.

SolarWinds' customers include most Fortune 500 companies, and it's U.S. government clients are rich with generals and spymasters.

The difficulty of extracting the suspected Russian hackers' tool kits is exacerbated by the complexity of SolarWinds' platform, which has dozen of different components.

"This is like doing heart surgery, to pull this out of a lot of environments," said Edward Amoroso, CEO of TAG Cyber.

Security teams then have to assume that the patient is still sick with undetected so-called "secondary infections" and set up the cyber equivalent of closed-circuit monitoring to make sure the intruders are not still around, sneaking out internal emails and other sensitive data.

That effort will take months, Alperovitch said.

If the hackers are indeed from Russia's SVR foreign intelligence agency, as experts believe, their resistance may be tenacious. When they hacked the White House, the Joint Chiefs of Staff and the State Department in 2014 and 2015 "it was a nightmare to get them out," Alperovitch said.

The U.S. Treasury Department building viewed from the Washington Monument, Wednesday, Sept. 18, 2019, in Washington. Hackers got into computers at the U.S. Treasury Department and possibly other federal agencies, touching off a government response involving the National Security Council. Security Council spokesperson John Ullyot said Sunday, Dec. 13, 2020 that the government is aware of reports about the hacks. (AP Photo/Patrick Semansky, file)

"It was the virtual equivalent of hand-to-hand combat" as defenders sought to keep their footholds, "to stay buried deep inside" and move to other parts of the network where "they thought that they could remain for longer periods of time."

"We're likely going to face the same in this situation as well," he added.

FireEye executive Charles Carmakal said the intruders are especially skilled at camouflaging their movements. Their software effectively does what a military spy often does in wartime—hide among the local population, then sneak out at night and strike.

"It's really hard to catch some of these," he said.

Rob Knake, the White House cybersecurity director from 2011 to 2015, said the harm to the most critical agencies in the U.S. government—defense and intelligence, chiefly—from the SolarWinds hacking campaign is going to be limited "as long as there is no evidence that the Russians breached classified networks."

During the 2014-15 hack, "we lost access to unclassified networks but were able to move all operations to classified networks with minimal disruptions," he said via email.

The Pentagon has said it has so far not detected any intrusions from the SolarWinds campaign in any of its networks—classified or unclassified.

Given the fierce tenor of cyberespionage—the U.S., Russia and China all have formidable offensive hacking teams and have been penetrating each others' government networks for years—many American officials are wary of putting anything sensitive on government networks.

Fiona Hill, the top Russia expert at the National Security Council during much of the Trump administration, said she always presumed no government system was secure. She "tried from the beginning not to put anything down" in writing that was sensitive.

"But that makes it more difficult to do business."

Amoroso, of TAG Cyber, recalled the famous pre-election dispute in 2016 over classified emails sent over a private server set up by Democratic presidential candidate Hillary Clinton when she was secretary of state. Clinton was investigated by the FBI in the matter, but no charges were brought.

"I used to make the joke that the reason the Russians didn't have Hillary Clinton's email is because she took it off the official State Department network," Amoroso said.